Korporativna varnost

ICS
Institut za korporativne varnostne študije

Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!

Letnik 2014, december • št. 8



Odgovornost korporativno varnostnega managerja

G. Štefan Gostič, TNT Expres Worldwide

6. mednarodna konferenca Dnevi korporativne varnosti

Ljubljana, 18.-19. marec 2015

Slovenian Grand Security Award 2014



Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki bo podeljena izbranim institucijam in posameznikov za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne varnosti.

Neodvisna komisija ocenjuje in izbira kvaliteto in izvirnost prijavljenih udeležence v naslednjih kategorijah:

Najbolj varno mesto
Najbolj varno podjetje
Najbolj inovativna varnostna rešitev
Korporativno varnostni manager leta
Najboljša knjiga s področja varnosti
Inovativna medijska promocija varnosti.

www.ics-institut.si



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

Glavni in odgovorni urednik:
dr. Denis Čaleta

Namestnik odgovornega urednika:
Andrej Kovačič

Trženje:
ICS-Ljubljana
info@ics-institut.si
Aljoša Kandžič
aljosa.kan@ics-institut.si

Oblikovanje in DTP:
ICS-Ljubljana

Tisk:
Schwarz print d.o.o.

Datum izida
december 2014

Izvod revije je brezplačen

Naslovnica in slike:
© Dreamstime.com

ISSN 2232-6170

Objavljeni prispevki in njihova vsebina odraža mnenja in stališča avtorjev ter predstavljajo v celoti njihovo odgovornost.

Počasi vendar dovolj očitno so se začele v poslovnem svetu nakazovati razlike v uspešnosti podjetij, ki so pogojene tudi z zavedanjem strateškega vodstva o potrebnosti učinkovitega obvladovanja tveganj. Ugotavljamo lahko, da je med uspešnimi podjetji več takih, ki imajo jasno opredeljeno lastniško strukturo, katero sestavljajo odgovorni lastniki, ki jim je skrb za njihovo premoženje oz. investicije zelo pomembna. Seveda so podjetja, ki so mednarodno vpeta, bila v svoji razvojni fazi primorana izpeljati ustrezne strukturne spremembe, ki so nedvomno vključevale tudi transformacijo procesov povezanih s celovitim obvladovanjem varnostnih tveganj za delovanje organizacije. Imamo tudi primere tujih korporacij, ki so lastniško vstopile v domača podjetja in skozi prenos svoje organizacijske kulture in procesov prisilile lokalna podjetja k drugačnim pristopom na omenjenem področju. Če pa situacijo v Sloveniji pogledamo v celoti, lahko ocenimo, da je stanje na področju zagotavljanja korporativne varnosti še vedno relativno slabo razvito. Predvsem so v večini primerov najbolj problematična podjetja, kjer je država večinski lastnik. V teh podjetjih se zelo močno transformira realno stanje družbe, ki se odraža skozi nizko stopnjo varnostne kulture, odsotnost kritičnega stališča do korupcije in drugih deviantnih ravnanj. Še posebej nas lahko v tem okviru skrbijo podjetja, ki v svojem okviru upravljajo s kritično infrastrukturo, katera je nujno potrebna za nemoteno delovanje širše družbene skupnosti v Sloveniji.

Strateška vodstva se v teh organizacijah ne zavedajo ali pa nočejo zavedati pomena tega ključnega procesa v njihovi organizaciji. Prepuščanje stihijskim rešitvam so predvsem hazardiranje, ki je v končni posledici v večini primerov obsojeno na večje škodne dogodke, odtekanje ključnih informacij in kadrov iz takih podjetij in v končni posledici tudi stagnacijo ali propad takih podjetij. Vodilnemu managerju, ki zaradi konsolidacije in racionalizacije procesov ukine delovno mesto korporativnega varnostnega managerja v svojem podjetju, na žalost ni mesta na odločevalskem nivoju, saj v osnovi ne razume dinamičnega varnostnega okolja v katerem deluje njegova organizacija.

Seveda pa ima v tem okviru svoj del odgovornosti tudi trenutni korporativno varnostni management, ki nima dovolj znanja in prodornosti za ustrezno predstavitev vseh pozitivnih učinkov, ki sledijo urejenemu procesu korporativne varnosti v podjetju. Od strateškega managementa pričakujemo, da bodo pri kadrovanju na mestih povezanih s korporativno varnostjo prenehali s prakso nekritičnega postavljanja oseb, ki prihajajo iz struktur državnih organov kot so policija in druge organizacije. Na žalost je v teh primerih odsotnost znanj, ki so potrebna za učinkovito upravljanje procesov korporativne varnosti tako velike, da v določenih primerih taka oseba naredi nepopravljivo škodo ugledu in strokovnim rešitvam v podjetjih. To dejstvo, da se raven korporativne varnosti nahaja zelo nizko v upravljalski strukturi podjetij, lahko med drugim pripišemo tudi zgoraj navedenemu dejstvu.

Na Institut za korporativne varnostne študije so pričela prihajati povpraševanja po korporativnih varnostnih strokovnjakih, ki jih potrebujejo za prosta delovna mesta v okviru mednarodnih korporacij. Tukaj bo priložnost za diplomante magistrskega programa »Mnagementa korporativne varnosti«, da pokažejo ali je njihovo znanje dovolj kvalitetno in konkurenčno za opravljanje nalog na tako zahtevnih delovnih mestih.

Pomembno je zavedanje, da se ebola, kibernetska tveganja, terorizem, poslovno vohunstvo in še vrsto drugih groženj nikakor ne ustavi na mejah naše države. Če na njih nismo ustrezno pripravljeni nas lahko hitro doleti, da bo ta odsotnost zavedanja izstavila račune, ki jih ne bo mogoče poravnati brez drastičnih posledic.

Doc. dr. Denis Čaleta
Glavni urednik



INTERVJU
mag. Miran Vršec
Inštitut za korporativne varnostne študije, Ljubljana

VARNOSTNIKI Z MINIMALNIMI PLAČAMI SO TVEGAN POSEL 11



ODGOVORNOST KORPORATIVNO VARNOSTNEGA MENEDŽERJA

Trenutno okolje v katerem poslujejo domače in mednarodne gospodarske družbe, je postalo kompleksno okolje negotovosti in poslovnih tveganj, v katerem so prisotne številne nevarnosti, pa tudi poslovne priložnosti. 16



VODSTVENI NADZOR V PROCESU UPRAVLJANJA KORPORATIVNE VARNOSTI

Morda je pravi čas, da v okviru tematik, ki jih obravnava revija Korporativna varnost spregovorimo tudi o vodstvenem nadzoru kot pomembnem dejavniku v procesu upravljanja korporativne varnosti. 24



VARNOST NA INTERNETU - NAJŠIBKEJŠI ČLEN JE UPORABNIK

V zadnjih letih opažamo velik porast spletnih prevar, ki ciljajo na podjetja. Goljufi v skrbno sestavljenih sporočilih obljubljalo neverjetne poslovne priložnosti, ki lahko podjetnikom pomagajo v težkih časih. 38



»BYOD« IZ PERSPEKTIVE NADZORA IN ZASEBNOSTI

V zadnjih letih se je na področju informacijsko komunikacijske tehnologije (IKT) ob konceptih računalništva v oblaku in interneta stvari, vse pogosteje začel uveljavljati izraz BYOD. Gre za kratico, ki v angleškem jeziku pomeni »(B)ring (Y)our (O)wn (D)evice«, ali po naše, »prinesi svojo napravo.« 41

Avtorja: izr. prof. Ddr. Teodora Ivanuša, Gašper Hribar, mag. var. /
Fakulteta za logistiko





NALEZLJIVE BOLEZNI IN VARNOST – nuja po zadostni in potrebni celovitosti, sistemskim razmišljanjem ter družbeno odgovornostjo

Človeštvo se sooča in živi s krizo izobilja, ki vsiljuje hedonizem in v povezavi z njim oziroma tudi z njim zlorabo drog, alkohola in drugih opojnih substanc, moralnih vrednot, skratka omama za vsako ceno, ki polni prazni prostor in čas brez vsebine. Človeštvo se sooča tudi z naravnimi ali drugačnimi krizami, med katerimi so 'nevidne krize' izbruhi nalezljivih bolezni, večina reakcij / akcij pa je takšna, ki ustreza 'fenomenu zanikanja' in oholosti: »Nam pa se kaj takšnega resnično ne more zgoditi...«

Pristojne institucije nas že leta (izbruh Aviarne influence, Nove gripe, Prašičje kuge, Ebola etc.) notorično 'mirijo', da je stopnja tveganja v Republiki Sloveniji nizka... Dejansko torej priznavajo, da tveganje obstaja, nihče pa ne pove ali pa ne zna povedati, kako 'nizko' je to tveganje, ki ga nevede priznavajo v imenu notoričnega pomirjanja in klicanja: 'Ostanimo trezni ...?'

Zagotavljanje varnosti je odvisno od individualne percepcije tveganj / groženj / nevarnosti, finančnih / človeških virov in drugih, relativno ambivalentnih okoliščin, kjer se neformalno sistemsko razmišljanje lahko pojavlja in se, vendar le delno in nezadostno.

Strateški načrti za izbruh nalezljivih bolezni niso niti sistematični, ne sistemski, saj izbrani vidiki obravnavanja ne ponujajo celovitega pristopa. Zanimivo je, da pristojne institucije glede izbruhov nalezljivih bolezni ne čutijo potrebe po kreativnem interdisciplinarnem sodelovanju glede varnosti, niti se varnostna stroka ne čuti poklicano za tovrstno sodelovanje ali pa pri poskusih tovrstnega sodelovanja naleti na izključevanje in ne dopolnjevanje.



Obvladujmo obvladljivo, preden pride do neobvladljivega, na kar pa pretežno ne moremo vplivati.

Zato je varnostna politika glede nalezljivih bolezni generalno odvisna le od subjektivnih izhodišč, osebnih interesov posameznikov v določenih institucijah, 'lastninjenja' problema, (vse dokler do problema dejansko ne pride in lastnika problema kar naenkrat 'čudežno' ni več ... ali pa se odgovornost s pristojnih institucij prenese na tiste, ki se jim je v procesu priprave načrtov / opomnikov / postopkovnikov ta domena grobo odvzemala ...) konfliktov idr., kar je precej zaskrbljujoče.

Nejasno opredeljeno (= fuzzy) je vse tisto, kar ni 100 % opredeljivo (Zadeh, 1965), torej skoraj vse, tudi nalezljive bolezni in predvsem varnost v povezavi z njimi, varnost ljudi. Edward Norton Lorenz (v Danforth, 2013) je kaos pojasnil: »Sicer sedanjost determinira bodočnost, toda približna / okvirna sedanjost niti približno niti okvirno ne determinira bodočnosti.« V znanstvenem kontekstu ima beseda kaos rahlo in zagotovo drugačen pomen, kot se sicer široko uporablja in razume, tj. kot stanje zmedenosti, pomanjkanja reda. Kaos v Teoriji kaosa se sklicuje na očitno pomanjkanje reda v sistemu, ki pa kljub vsemu delno uboga zakone oziroma pravila; takšno pojmovanje kaosa je sinonimno z dinamično nestabilnostjo, stanjem, ki ga je odkril in opisal francoski fizik, matematik in filozof Henri Poincaré (1854-1912) v zgodnjih letih 20. stoletja in se sklicuje / nanaša na inherentno pomanjkanje predvidljivosti v nekaterih fizikalnih sistemih. V znanstvenem kontekstu zato o kaosu v Teoriji kaosa v varnosti ne govorimo, prej je verjetnejši tisti, drugačen pomen: stanje zmedenosti, pomanjkanje reda, kot posledica enostranskosti in pomanjkanja zadostne in potrebne celovitosti, sistemskega razmišljanja in družbene odgovornosti. Dve osrednji komponenti Teorije kaosa, ki sta ideji: (1) da se sistemi, ne glede na to kako kompleksni bi naj bili, oziroma to dejansko so, zanašajo na svojo strukturno podstat oziroma red; in (2) da so zelo enostavni sistemi in dogodki lahko vzrok zelo kompleksnim obnašanjem in dogodkom. Slednja ideja je znana kot občutljiva odvisnost od inicialnih / začetnih okoliščin; okoliščina, ki jo je odkril in opisal Edvard Norton Lorenz (1917-2008), znan in priznan kot pionir na področju Teorije kaosa v zgodnjih 60. letih. Mulej in sod. (2000: 52) so zato slikovito razložili, da »[...] kjerkoli je možnih več variant odločitve, so razmere kaotične. Torej je kaos zelo naraven, ne pa problematičen ali celo odpravljiv, je pa težaven,« in dodali (ibidem), da so »kaotični tisti procesi, ki so v svojem ravnanju *delno deterministični* in delno *ne-deterministični*, torej delno (ne)predvidljivi [...] *Življenje je pač nelinearno in to velja tudi za skoraj vse drugo, kar je vredno zanimanja*.« Richards (v Kiel, Elliot, 1997; v Mulej et al., 2000: 54) je ugotovil: »Zaradi mešanice reda in kompleksnosti je – za trdo-sistemsko, newtonsko razmišljanje – Teorija kaosa neobičajen teoretični okvir.«

Zahteva namreč, da razmišljamo sistemsko, kajti *tradicionalna* obravnava po delih in s seštevanjem spoznanj iz delnih raziskav, *ni uporabna:* celota objekta se v resnici ne da razstaviti na dele, ki ne vplivajo drug na drugega.« Mulej et al. (ibidem: 55) opisujejo »teorijo kompleksnosti kot novejši korak v isto smer (= most med strokami, poklici, praksami),« in dodajajo: »Medsebojne vplive in emergentne sinergije so v preteklosti spregledali ali morda celo namenoma pustili ob stran, da bi zmogli priti vsaj do spoznanj o posamičnih delih stvarnosti, **naravoslovnih, tehniških in družbenih**. Dejansko seveda ne gre za tri stvarnosti, ampak za tri *vidike,* na katere se opazovalci, raziskovalci in obvladovalci osredinijo, da bi iz celote dogajanja izluščili nekaj, kar štejejo za posebej zanimivo. Svet bi bil sicer videti preveč zapleten, da bi ga bilo mogoče obvladovati.« Zato zaključijo (ibidem: 56), da je »*bi-*





stvena sposobnost videti povezave, soodvisnosti, medsebojne vplive, ne samo delov brez povezav.« Mulej et al. (ibidem: 57) pravijo: »Vedno gre za kompleksnost (= *zapletenost zaradi odnosov med sestavinami*).«

Kako vse to povezuje oziroma izključuje nalezljive bolezni in varnost, ki se strogo ločujeta oziroma se razumeta vsaj na dva zelo pogosta načina: (1) varnost in varnostne storitve normalno in pričakovano zagotavljajo varnost; (2) skrbi za varnost pa glede nalezljivih bolezni oziroma njihovih posledicah posebej, tj. dodatno, ne potrebujemo, ker bi morebitno potrebovanje dodatne varnosti (= ki je izven pričakovane) pomenilo priznanje 'nevarnosti'. Ali slikoviteje, dobro je tako dolgo: »Ko se zgodi skoraj, ne zares.« (Mulej & Jevtič, 2013, osebni vir).

Totalne celovitosti ali kaotičnosti ni, lahko pa je zadostna in potrebna celovitost, ker fuzzy ni le teorija, je dejstvo, kaos in kompleksnost prav tako; pot do nje je stvar sistematičnega in sistemskega pristopa v preventivi, predvsem v preventivi. Obvladujmo obvladljivo, preden pride do neobvladljivega, na kar pa pretežno ne moremo vplivati. Bolje, a pogosto preveč enostavno, je sicer misliti, verjeti v koncept: »'Meni se ne more nič zgoditi'. 'Naj se ne bi', bi bil boljši dialektični sistem vidikov oziroma izhodišče. 'Vemo, da ne moremo vsega vedeti; upravljamo, ne da se da vse upravljati'; nihamo med obvladovanjem in neobvladovanjem.« (Mulej et al., 2000; po Flood, 1999)

Zanimajo nas vidiki obravnavanja / razumevanja varnosti glede nalezljivih bolezni (= iščemo sinergije oziroma njihovo odsotnost), kot tudi tipi nevarnosti in želje / percepcije ljudi ter vpliv njihovih osebnosti na percepcijo varnosti med realnostjo in iluzijo. Pri tem upoštevamo tudi fuzzy logiko (Zadeh, 1988: 83-84), ki prej kot v eksaktnem, leži v približnem, v načinu razmišljanja, njena aplikativnost pa ima razpon, ki se razteza vse od procesov nadzora do medicinskih diagnoz. Za razliko od klasične logike, fuzzy logika temelji na modeliranju nenatančnih oblik pojmovanja, ki igrajo esencialno vlogo v čudoviti človeški sposobnosti za sprejemanje racionalnih odločitev v okoliščinah / okolju negotovosti in netočnosti. Ta sposobnost je izmenoma odvisna od naših sposobnosti sklepanja in približnih odgovorov na vprašanje, ki temelji na zakladnici znanja, ki ni točno, ni popolno in povsem zanesljivo. Zadeh (ibidem) navede nekaj takšnih primerov: »(1) po navadi traja pot iz Berkeleyja do Stanforda približno eno uro in približno pol ure vožnje od Stanforda do San Jose-ja.

Splošne ocene pristojnih institucij za nalezljive bolezni o varnosti namreč nimajo prav veliko skupnega s preventivnim ocenjevanjem varnostnih tveganj v varnostnem menedžmentu ali preprosteje, s preventivo na tem področju. Končni rezultat, torej absolutna varnost, kot jo ocenjujejo / zaznavajo pristojne institucije za nalezljive bolezni, ima v varnostnem menedžmentu bistveno drugačno topografijo oziroma hierarhijo zaporedja in soodvisnosti.



Kako dolgo bi trajala vožnja iz Berkley-ja do San Jose-ja preko Standforda? (2) Velika večina tistih, ki živijo na Belvederu, imajo visoke prihodke. Možno je, da Mary živi na Belvederu. Kaj lahko rečemo o Marynih prihodkih? (3) Vitkost je atraktivna. Carol je vitka. Je Carol atraktivna? (4) Brian je veliko višji kot večina njegovih prijateljev. Kako visok je Brian?«

Podobno kot Zadeh tudi sami navajamo nekaj trditev in vprašanj, ki dajejo fuzzy odgovore:

- Priporoča se, da se naj ljudje zaradi osebne varnosti izogibajo potovanjem v države, kjer je prišlo do izbruha nalezljive/ih bolezni. Ali le oziroma tudi dosledno izogibanje tovrstnim potovanjem pomeni osebno varnost?
- Priporoča se preventivno cepljenje pred odhodom na določene destinacije. Ali sta npr. hepatitis A in B stvar destinacije ali neukosti oziroma nevarnih postopkov in odločitev posameznika?
- Trdi se, da ima določena destinacija nizko / visoko ogroženost za nalezljive bolezni. Kako nizka / visoka oziroma posledično varna je dejansko ta destinacija?
- Varnostna kultura ljudi pomembno vpliva na njihovo osebno varnost na sicer že varnih destinacijah. Kako velik je ta vpliv in kaj / koliko pomenita beseda 'sicer' in 'že'?
- Priporoča se, da naj si ljudje redno umivamo roke, kihamo v rokav, kašljamo v robček, ki ga kasneje zavržemo, si razkužujemo roke etc. Je to dovolj, premalo ali edino, je to tisto, kar definira magnitudo tveganja?

Obstajata vsaj dva osrednja razloga, zakaj se klasična logika ne more spopadati s tovrstnimi problemi: (1) ti problemi ne zagotavljajo predstavitvenega sistema za pomen teh predpostavk, izraženih v naravnem / vsakodnevnem jeziku, ko je pomen nejasen, in (2) v primerih, ko se pomen lahko izraža kot simboličen / simbolika s pomenskim, reprezentativnim jezikom, npr. kot semantična mreža ali konceptualno-odvisni grafi, ni mehanizma za sklepanje. Fuzzy logika tovrstne probleme obravnava na naslednja načina: (1) pomen besedno netočnih predpostavk je predstavljen kot elastična omejitev na variabli in (2) odgovor na vprašanje je izpeljan s propagiranjem elastičnih omejitev (ibidem).



Stuart Umpleby (Umpleby, 1991), eden od arhitektov kibernetike, je menil, da so razprave o vseh temah (= tudi o varnosti in varnostnem menedžmentu) lahko koristne, vendar je menil tudi, da bodo najbolj plodne tiste razprave, ki bodo obravnavale fundamentalne teme / probleme; probleme, kjer ljudje preveč jemljejo za samo po sebi umevno dejstvo, da niti pomislili niso, da bi lahko drugi ljudje mislili drugače.

Pristojne institucije za nalezljive bolezni in njihovi odgovorni glasniki se pogosto oklepajo relativno pavšalnih in enostranskih varnostnih ocen ter podatkov, objavljenih na uglednih svetovnih forumih, ki mirijo bodoče in aktualne deležnike, češ, da je varno. Zdi se, da je vse zadostno in potrebno celovito. Je tudi v stiku z realnostjo zares tako, ali se zdi umestno in modro vsaj poznati oziroma upoštevati dihotomije?

Splošne ocene pristojnih institucij za nalezljive bolezni o varnosti namreč nimajo prav veliko skupnega s preventivnim ocenjevanjem varnostnih tveganj v varnostnem menedžmentu ali preprosteje, s preventivo na tem področju. Končni rezultat, torej absolutna varnost, kot jo ocenjujejo / zaznavajo pristojne institucije za nalezljive bolezni, ima v varnostnem menedžmentu bistveno drugačno topografijo oziroma hierarhijo zaporedja in soodvisnosti.

Običajno se znanstveno-strokovna razprava varnostnega menedžmenta o varnosti in pri njegovih odgovornih glasnikih razume kot 'grožnja' varnosti, kar ni v duhu prepričanja, da je potrebno sprejeti druge, drugi pa imajo pravico in dolžnost biti drugačni. Še več, ta reakcija je povsem v nasprotju s pričakovanim odzivanjem odraslih in odgovornih, razen če pri tem ne poskušamo razumeti in dojeti 'vonja po denarju' za vsako ceno. Ali če parafraziramo Zadeha (1988) in rečemo / vprašamo: »Varnost glede nalezljivih bolezni je na visoki ravni. Kako visoka pa je ta raven?« Lahko le ugibamo!

Če dovolj zanesljive rešitve ni, se kaže lotiti problema kot nečesa, kar potrebuje inovacijo.

Spomnimo na pravila (Mulej et al., 2008) Procesnega modela invencijsko-inovacijskega difuzijskega procesa, IIDP (povratne zveze neupoštevane), in na Okvirni model spiska soodvisnih pogojev za uspeh IIDP (podrobnosti in sinergije neupoštevane), ki utegneta pristojnim za nalezljive bolezni utemeljeno predlagati intenzivnejše sodelovanje z varnostnim menedžmentom in percepcijo le-tega kot strateškega orodja v fazah načrtovanja oziroma preventive in predvsem preventive. Nihče iz varnostne stroke ne pričakuje te potrebe kot potrebe, da o njej v celoti obveščamo javnost, ki bi to interdisciplinarnost lahko razumeli / dojemali kot nevarnost. Namreč, preventiva in samo preventiva lahko definira 'višino' varnosti, ki je sicer stvar dihotomije, fuzzy logike...

In kdo si v času 'krize izobilja', ki hromi kreativnost, še upa dopovedovati, dokazovati, da je preventiva stvar inercije, celo slučaja? Kdo še stavi na odsotnost kompliciranega in zaradi enostranskosti prehoda komplikacij v kompleksno? Vsaj zakon zadostne in potrebne celovitosti in družbena odgovornost takšnih stav / neodgovornosti ne sprejemata.

Slika 1: Procesni model IISPIIDP (povratne zveze neupoštevane) (Mulej, 2013, osebni vir)

IDEJE	→	INVENCUJE	→	SUGESTIJE	→	POTENCIALNE INOVACUJE	→	INOVACIJE	→	DIFUZIJA
OBETAVNE		ZAPISANE		RAZVITE		V UPORABI		PRI MNOGIH		KORIST MNOGIH
NEOBETAVNE	→?	NEZAPISANE	→?	NERAZVITE	→?	NISO V UPORABI	→?	NISO PRI MNOGIH	→?	NI KORIST MNOGIH

Splošne ocene pristojnih institucij za nalezljive bolezni o varnosti namreč nimajo prav veliko skupnega s preventivnim ocenjevanjem varnostnih tveganj v varnostnem menedžmentu ali preprosteje, s preventivo na tem področju.



Veliko je idej, toda le ena od približno tisočih postane inovacija, tj. praktično preverjena in vsebuje prednosti za uporabnike. Nekatere ideje imajo potencial za nove prednosti in se imenujejo invencije. Nekatere invencije so zabeležene, pa vendar pozabljene in se lahko imenujejo predlogi. Nekatere od njih so podvržene difuziji za mnoge uporabnike in ustvarjajo nove rutine. Te nove rutine in njihov ne-aplikativni potencial vseh predhodnih faz pa omogočajo nov idejno-invencijski- predlagalni potencial invencijsko-inovativnih difuzijskih procesov, ki potekajo neprekinjeno.

Uspeh teh dolgih, zapletenih in kompleksnih procesov je odvisen od zadostne in potrebne celovitosti v vsaki fazi procesa posebej, profesionalizmu, kreativnem interdisciplinarnem delu, ki temelji na sinergijah vseh sposobnostih in zmogljivostih.

V danem primeru, nalezljive bolezni in varnost, se vsi rezultati nanašajo na vse ključne profesije / poklice v vseh ključnih fazah procesa; na vse ključne tipe potencialnih tveganj / groženj / nevarnosti, kot so nalezljive bolezni, vse do epidemije in pandemije.

Vsa ta tveganja / grožnje / nevarnosti zahtevajo upravljanje in obvladovanje / aplikacijo preventive pri vseh deležnikih in potrebo / zahtevo, da v imenu zadostne in potrebne celovitosti upoštevajo naslednje kriterije:

Slika 2: Okvirni model spiska soodvisnih pogojev za uspeh IIDP (podrobnosti in sinergije neupoštevane) (Mulej, 2013, osebni vir)

Menedžmenski pogoji	Pogoji znanja in vednosti	Pogoji vrednot, kulture, etike, norm	Pogoji obnašanja	Neosebni pogoji	Pogoji trga
IIDP v spletu	Znanje, vednost, strokovnost	Motivacija	Zadostna in potrebna celovitost obnašanja, zato dolgoročno in široko razmišljanje in obnašanje, da prepreči visoko ceno kratkoročnih in ozkih odločitev	Materialni, naravni, ekonomski, ekološki ipd. pogoji	Dojemanje in razvoj ter predvidevanje (prednostnih) potreb možnih novih in stalnih odjemalcev, pa tudi avtorjev in lastnikov novosti (posledično)
- Vizija	- Izrecno	Vrednote, kultura, etika in norme za IIDP			
- Misija	- Prikrito				
- Politika	- Obvladovanje - vodenje znanje idr.	Zanesljivost in zaupanje	Odprto inoviranje, le delno zaprto	Dojemanje in razvoj lastnih sposobnosti in možnosti	Odkrivanje praznin na trgu in polnjenje le-teh (z RR, marketingom, antropologi, etnologi itd.)
- Strategija/e					
- Taktika/e	Ustvarjanje				
- Operativa	Učenje	Etika soodvisnosti	Tržni pritisk predviden		
- Podatkovno spremljanje	Sodelovanje	Srečnost in dobro počutje s pomočjo IIDP		Ustvarjanje pogojev in priložnosti	Povezava IIDP s poslovno odličnostjo in zato z družbeno
- Povratni vplivi/ posegi	Mreženje	Upoštevanje 5l "integracije, imaginacije, involviranja, intelekta in intervencije"		Upoštevanje celotne enačbe pogojev za nastanek inovacije	
Sodelovalno namesto enosmerno ukazovalno	Vsrkavanje znanja idr.				
Podjetnost (pomembnejša od lastništva)					
Obvladovanje celotna enačbe pogojev za inovacijo					



In ne gre za klasičen članek, gre za uvodno razmišljanje in drobne predloge za upravljanje in obvladovanje nalezljivih bolezni kot kritičen segment korporativne varnosti. Kajti nalezljive bolezni, npr. Ptičja gripa, lahko resno in celo katastrofalno prizadenejo prehransko industrijo, perutninarstvo, matično jato, oskrbo s hrano in posledično celotno ekonomijo / gospodarstvo Republike Slovenije in regije...

Literatura in viri

- Danforth, C. M. (2013). Chaos in an atmosphere hanging on a wall. *Mathematics of Planet Earth,* najdeno 22.11.2014 na http://mpe2013.org/2013/03/17/chaos-in-an-atmosphere-hanging-on-a-wall/
- Mulej, M., Espejo, R., Jackson, M., Kajzer, S., Mingers, J., Mlakar, P., Mulej, N., Potočan, V., Rebernik, M., Rosicky, A., Schiemenz, B., Umpleby, S., Uršič, D. & Vallee, R. (2000). *Dialektična in druge mehkosistemske teorije (podlaga za uspešen*
- Mulej, M. et al. (2008). *Invencijsko-inovacijski management z uporabo dialektične teorije sistemov (podlaga za uresničitev ciljev Evropske unije glede inoviranja*. Ljubljana: Inštitut za inovacije in tehnologijo Korona Plus d.o.o.
- Umpleby, S. A. (1991). Strategies for Winning Acceptance of Second Order Cybernetics. V G. E. Lasker et al. (ur.), *Advances in Human Systems and Information Technologies* (str. 97-196). Windsor: International Institute for Advanced Studies in Systems Research and Cybernetics.
- Zadeh, L. A. (1965). Fuzzy Sets. *Information and Control,* 8, 338-353.
- Zadeh, L. A. (1988). Fuzzy Logic. *Computer*, 21 (4), 83-93. ■

Avtor: GEA College / Fakulteta za podjetništvo*

INTERVJU
mag. Miran Vršec
Inštitut za korporativne varnostne študije, Ljubljana

VARNOSTNIKI Z MINIMALNIMI PLAČAMI SO TVEGAN POSEL

Varnostne službe so postale temelj varnega in učinkovitega delovanja podjetja, vendar na tem področju najemniki varnostnih služb velikokrat grešijo že v izhodišču, že pri sami izbiri primerne varnostne službe.

Najem varnostne službe, ki bo varovala imetje našega podjetja in s tem nemalokrat pripomogla celo k uspešnosti njegovega delovanja v poslovnem okolju, je strateškega pomena. Kljub temu pa se prepogosto dogaja, da se izbira primerne varnostne službe izvaja na podlagi napačnih meril, najpomembnejša je še vedno najnižja cena.

To pa je samo eno od pomembnih tveganj, s katerimi se v zadnjih letih srečujejo slovenska podjetja. O tem, kako povečati varnost v podjetjih, in o tem, kako pomembno je izobraževanje kadrov na tem področju, smo se pogovarjali z Miranom Vršcem, uspešnim podjetnikom, ki ima v lasti družbo za integrirano varovanje Nova Panorama in je predsednik upravnega odbora združenja Alumni klub GeaCollege ter predavatelj novega podiplomskega programa Management korporativne varnosti na Fakulteti za podjetništvo GeaCollege.

Kako menite, da se skozi čas spreminjajo tveganja, ki so jim izpostavljena slovenska podjetja?

Zaznavamo, da trenutna kriminalna tveganja v podjetjih izhajajo predvsem iz socialnih stisk zaposlenih. Seveda je ta izpostavljenost odvisna od dejavnosti posameznega podjetja. Če za primer izpostavimo problematiko varovanja v trgovskih središčih, so se izredno povečale tatvine prehrambnih izdelkov, izdelkov za osebno uporabo in izdelkov, ki se jih lahko na hitro proda na črnem trgu. Vse več je primerov, ko stranke prehrambne izdelke pojejo že v trgovini. Povečano stopnjo izpostavljenosti krajam zaznavamo tudi na območjih skladišč in na logističnih poteh, po katerih se prevaža blago. Če pa pogledamo malo širše, se ta problematika širi na krajo intelektualne lastnine ter poslovnih in preostalih podatkov, ki so ključnega pomena za podjetja. Posamezniki povzročajo škodo določenim podjetjem zaradi osebnih zamer ali iz golega koristoljubja, organizirane skupine pa predvsem zaradi pridobitve poslovnih koristi in/ali povzročanja poslovne škode.V velikem porastu je tako imenovani „cyber“ kriminal, ki je ena največjih sodobnih groženj poslovanju podjetij.

> Zasebno varovanje je dejavnost, ki temelji na zaupanju, zaupanje pa lahko na dolgi rok gradiš tudi tako, da imaš zadovoljne in lojalne zaposlene. Če zaposleni, torej varnostniki, niso zadovoljni in, če niso lojalni, si zgrešil bistvo te dejavnosti.

V kakšno nevarnost se spušča podjetje, ki najema zunanja varnostna podjetja?

Opažam, da je največja težava ta, da naročniki izvajalce še vedno izbirajo večinoma na podlagi najnižje cene. Cena je glavno merilo. Kljub našemu velikemu angažiranju in angažiranju Inštituta za korporativne varnostne študije, da ozaveščа naročnike o tej problematiki, še vedno ugotavljamo, da na tem področju ni bistvenih sprememb. Dejstvo je, da je še vedno najlažje izbrati izvajalca po merilu najnižje cene, saj je v tem primeru razpisno dokumentacijo dokaj preprosto pripraviti. Čim se začnejo spuščati v neke kompleksnejše razpisne pogoje, naročnikom praviloma zmanjka znanja ali pa se ne znajo obrniti na prave ljudi, ki bi jim znali svetovati, kako pripraviti razpisno dokumentacijo, ki bi zagotavljala izbor ekonomsko najugodnejšega ponudnika, ne pa cenovno najugodnejšega ponudnika.

*Vsebina objavljena tudi na spletnem portalu PLANET SIOL.NET.



Kakšna so slaba varnostna podjetja?

Zasebno varovanje je dejavnost, ki temelji na zaupanju, zaupanje pa lahko na dolgi rok gradiš tudi tako, da imaš zadovoljne in lojalne zaposlene. Če zaposleni, torej varnostniki, niso zadovoljni in, če niso lojalni, si zgrešil bistvo te dejavnosti. Največja težava je v tem, da ima večina varnostnega osebja minimalno plačo. V praksi se dogaja, da imajo zaposleni, ki so podvrženi nadzoru varnostnika, višjo plačo od njega. To nekako ne gre skupaj. Kako ima lahko tisti, ki nadzira, nižjo plačo od nekoga, ki je nadzorovan? Tukaj lahko nastane nasprotje interesov, zato so varnostniki pogosto izpostavljeni različnim poskusom podkupovanja, dogovarjanja in podobnim aktivnostim, ki jih lahko napeljujejo na izvajanje kaznivih dejanj. Poleg tega se je treba zavedati, da varnostnik z minimalno plačo težko preživi, posledično je vedno več varnostnikov obremenjenih s posojili in z raznimi izvržbami, kar še dodatno otežuje njihovo delo. V zadnjem času je vse več tudi osebnih stečajev varnostnega osebja. Po mojem mnenju takšni ljudje ne morejo sproščeno in maksimalno zbrano opravljati nalog varovanja. Pri tem je nujno treba izpostaviti to, da so plače varnostnega osebja vezane na ceno storitve, ki jo je pripravljen plačati naročnik. In če je naročnik pripravljen plačati minimalno, motivacija izvajalcev žal ne more biti na visoki ravni.

Kakšna je rešitev?

Poznam naročnike, ki so to težavo rešili tako, da so v razpisnih pogojih navedli, kakšno minimalno plačo mora imeti varnostnik, ki bo delal pri njih. Seveda to pomeni, da bo moral naročnik za storitve plačati več.

Kakšna bi morala biti potem tista prava merila, po katerih izberemo neko varnostno službo?

Meril je lahko kar nekaj. Težava je, da je treba pripraviti merila, ki niso diskriminatorna, so merljiva in jih je mogoče preveriti. Treba je upoštevati bonitetne ocene ponudnika in njegov ugled. Pomembna je tudi velikost podjetja, kakšni ljudje delajo v tem podjetju, kakšna je lastniška struktura, kakšne so njegove reference, kako se ponudnik loti reševanja varnostne problematike naročnika, ali je razvojno usmerjen in tako naprej. Po drugi strani pa, če gledamo varnostno osebje, lahko naročnik zahteva tudi določeno stopnjo izobrazbe varnostnega osebja, ne samo tiste osnove, ki je zakonsko predpisana. Lahko zahteva določene delovne izkušnje, določi starost ali spol varnostnika. Treba je preveriti, kakšne licence ima podjetje, s kom sodeluje in koliko časa je na trgu.

Težava je tudi v tem, da varnostne službe redko materialno in kazensko odgovarjajo za nespoštovanje oziroma kršitve pogodbenih obveznosti. Zadnje čase naročniki v vse manj primerih zahtevajo bančne garancije za kakovostno izvedbo pogodbenih obveznosti. V svoji več kot 20-letni praksi na področju zasebnega varovanja se ne spomnim primera v zasebnem varovanju, v katerem bi nekdo unovčil bančno garancijo zaradi slabe izvedbe ali kršitev pogodbenih obveznosti. Izvirni greh je v tem, da tudi tam, kjer bančne garancije za resnost ponudb so, kršitve pogodbenih obveznosti in način unovčevanja bančnih garancij niso dovolj dobro določeni, unovčenje bančne garancije pa je zaradi tega praktično nemogoče. Mislim, da je tukaj še veliko možnosti za izboljšave, in če bi se tudi ta segment uredil, bi verjetno kar nekaj izvajalcev lahko nehalo opravljati svojo dejavnost oziroma bi morali bistveno spremeniti svoj način delovanja in poslovanja.

Kako pa so zavarovalnice pozorne na te pomanjkljivosti?

Zavarovalnice pri nas so na tem področju v nekakšnem krču. Tuje poslovne prakse kažejo, da so zavarovalnice tiste, ki narekujejo, kakšne pogoje mora izpolnjevati njihova stranka, da ji bodo zavarovali premoženje. Zavarovalnice same izdelajo kompleksno analizo ranljivosti, ogroženosti in varnostnih tveganj ter same ugotovijo, kako oziroma na kakšni ravni in ali sploh podjetje obvladuje ranljivost, ogroženost in varnostna tveganja, ki se pojavljajo v njegovih poslovnih procesih in na lokacijah delovanja. Če podjetje za zavarovalnico predstavlja preveliko tveganje, zavarovalnica premoženja takemu podjetju ne bo zavarovala.V Sloveniji so zavarovalnice na tem segmentu precej podhranjene in bi lahko naredile bistveno več.Pri nas zavarovalni agentje preveč na hitro in na pamet zavarujejo premoženje ter se verjetno niti ne zavedajo, kakšno poslovno škodo lahko s tem povzročijo zavarovalnici.

S kakšnimi znanji boste opremili študente podiplomskega študijskega programa Management korporativne varnosti?

Naš interes je, da na trgu ponudimo znanja, ki so uporabna v praksi. Kandidati, ki bodo obiskali ta magistrski program, bodo bolj konkurenčni od preostalih. Ko smo snovali ta program, smo med drugim izhajali tudi iz predpostavke, da ta program lahko obiskujejo praktično vsi, ki so v menedžmentu. Program posredu-





je široka znanja iz menedžmenta, prava, načrtovanja varnostnih rešitev in sistemov varovanja, korporativne varnosti, ekonomike, standardov, zavarovalništva, ekologije, informatike in z drugih področij tako z lokalnega kot tudi globalnega vidika. S pridobljenim znanjem bodo naši študentje sposobni upravljati korporativno varnost na strateški ravni, znali bodo prepoznati, kje je podjetje ogroženo in ranljivo, znali bodo oceniti stopnjo ogroženosti in ranljivosti, verjetnost nastanka varnostnih pojavov ter sistemsko pristopali k obvladovanju vseh teh tveganj tako na operativni kot tudi strateški ravni. Temeljni cilj našega programa je ponuditi interdisciplinarna znanja, s katerimi bodo študentje sposobni upravljati tveganja v nekem korporativno-varnostnem okolju – ne samo v lokalnem okolju, ampak tudi globalno.

Ali svojo podjetniško žilico uporabljate tudi v odnosu do svojih študentov?

Ravno to je ena od prednosti našega programa. Vsi predavatelji izhajamo tudi iz prakse in prav s konkretnimi primeri študentom dokazujemo, kako se zadevam streže oziroma kaj vse se lahko v praksi zgodi, če se varnostna tveganja ne obvladujejo na strateški ravni. Naše praktične izkušnje, povezane s teoretičnimi znanji, so temelj za naše delo s študenti. Naš študij ni zgolj teorija, ampak je teorija, ki se povezuje s prakso. Pridobljena znanja bo tako mogoče uporabiti v praksi. Ravno zato smo se odločili, da Inštitut za korporativne varnostne študije kot snovalec programa stopi v partnerstvo s Fakulteto za podjetništvo GeaCollege. To je ena redkih slovenskih fakultet, ki dejansko ponuja praktična in uporabna znanja na področju podjetništva in menedžmenta. Drugo pomembno izhodišče pa je to, da bomo skozi študij lahko svoje študente povezali s konkretnimi naročniki in jim tako omogočali prakso, pozneje morda tudi zaposlitev.

Zakaj bi nekomu svetovali, da se vpiše na podiplomski študij?

Preprosto zato, ker je to edini magistrski program, ki študentom ponuja interdisciplinarna znanja s področja upravljanja korporativne varnosti in jim skozi študij zagotavlja gradnjo osebnih konkurenčnih prednosti na trgu delovne sile tako doma kot tudi v tujini. Prepričan sem, da bodo študentje po koncu študija izredno iskani in si bodo s pridobljenimi znanji lahko ustvarili ustrezen status v podjetjih, kjer bodo nadaljevali svojo poslovno kariero. ■

Nova panorama

družba za integrirano varovanje

www.novapanorama.si

Prvim desetim strankam, ki se bodo javile na elektronski naslov: *info@novapanorama.si* ponujamo brezplačno uro varnostnega svetovanja na temo kako optimizirati investicije v varnostni sistem in tekoče stroške financiranja varnostnega sistema?

IZVIRNA MISEL

Profesionalni in celovit varnostni sistem v podjetju odločilno prispeva k povečanju pozitivnih poslovnih izidov ter k dvigu kulture, konkurenčnih prednosti in ugledu podjetja (M. Vršec).

PRAVA IZBIRA

Nova Panorama, d. o. o. je ob sodelovanju vrhunskih varnostnih strokovnjakov usposobljena izvajati varnostni inženiring, to je varnost od A do Ž oziroma t. i. "varnost na ključ". Gre za vzpostavljanje integralnih varnostnih sistemov na projektni način, z integracijo varovanja v sisteme vodenja kakovosti z uvajanjem varnostnih standardov ter z upoštevanjem dobre prakse. Konkretni projektni proizvod je izdelava in implementacija varnostnega elaborata.

Storitve in produkti Nova Panorama, d. o. o. naročniku oziroma uporabniku zagotavljajo uvedbo varnostno in ekonomsko upravičenega varnostnega sistema, ki vzpostavlja ustrezno preventivo, opozorilni sistem in proces obvladovanja ranljivosti, ogroženosti, sprememb, tveganj in izrednih dogodkov.

GLAVNE DEJAVNOSTI

Poslovno-varnostno svetovanje

- Načini (oblike) svetovanja
- Posnetek in analiza stanja
- Intervjuji in vprašalniki
- Ocene ogroženosti
- Varnostni elaborati
- Pravilniki, načrti, navodila

Integralni varnostni sistemi (celovito varovanje)

- Varnostna funkcija
- Varnostna politika
- Varnostna strategija
- Pravna podlaga
- Organiziranost in status varovanja
- Področja varnosti
- Civilna zaščita
- Varnostni menedžment
- Varnostni režim
- Alarmni in odzivni sistem
- Strokovni nadzor
- Portfelj zavarovanj

Varovanje oseb in premoženja

- Varovanje ljudi premoženja
- Prevoz in varovanje denarja ter drugih vrednostnih pošiljk
- Varovanje javnih zbiranj

10 LET ODLIČNOSTI

- Izvajanje sistemov tehničnega varovanja

Kakovost in varnost

- Integracija varovanja v ISO 9000:2000
- Varnostni standardi
- Presojevalci kakovosti varovanja

Krizno vodenje (krizni menedžment)

- Objektivna potreba po načrtovanju kriznega vodenja
- Poslovanje na rezervni lokaciji

IZOBRAŽEVANJE

Varnostni menedžment

- Obvladovanje poslovnih in varnostnih tveganj ("risk management")
- Usposabljenje kriznega štaba
- Varnostna služba – usposobljenost varnostnikov za naloge varovanja podjetja
- Varnostna kultura in poslovna etika
- Usposabljanje za nadzornike
- Scenariji obvladovanja izrednih dogodkov



Avtor: Štefan Gostič, univ. dipl. pravnik / Vodja varnostne politike in Kadrovski direktor v podjetju TNT Express Worldwide, distribucija, d.o.o.*



ODGOVORNOST KORPORATIVNO VARNOSTNEGA MENEDŽERJA

Trenutno okolje v katerem poslujejo domače in mednarodne gospodarske družbe, je postalo kompleksno okolje negotovosti in poslovnih tveganj, v katerem so prisotne številne nevarnosti, pa tudi poslovne priložnosti.

Uvod

Podjetja poslujejo v poslovnem okolju, ki je medsebojno prepleteno in soodvisno, kar (lahko) posledično pomeni velik izziv za menedžerje, ko ocenjujejo nove poslovne priložnosti in s tem povezana tveganja. Učinkovito upravljanje oz. obvladovanje poslovnih tveganj je ena od osnovnih dolžnosti in odgovornosti poslovodstva. Nadzorni sveti družb in ključni deležniki (predvsem lastniki in javnost!) povsem upravičeno pričakujejo, da bodo gospodarske družbe ne samo ohranjale, temveč predvsem povečevale premoženje in ustvarjale dodatno vrednost, hkrati pa zagotavljale varno poslovanje; to pa predvsem pomeni obvladovanje tveganj in vzpostavitev ustrezne korporativne varnosti v podjetju. Slednje pa zahteva učinkovito vodenje (*Leadership*) in jasno opredelitev konkretnih pristojnosti in odgovornosti oseb(e), ki je odgovorna za stanje korporativne varnosti. Ta oseba je lahko korporativni varnostni menedžer, ki je lahko član organov vodenja družbe (uprave ali upravnega odbora). Učinkovito obvladovanje oz. upravljanje tveganj ter organizacijska vzpostavitev korporativne varnosti postaja imperativ pri poslovanju gospodarskih družb. Zagotavljanje nemotenega poslovanja družbe, ugleda v javnosti, nedotakljivosti premoženja ter zagotavljanje varnosti in zdravja pri delu, je v marsičem odvisno od opredeljenih odgovornosti (odgovornega dela!) korporativno varnostnega menedžerja.

Učinkovito obvladovanje oz. upravljanje tveganj ter organizacijska vzpostavitev korporativne varnosti postaja imperativ pri poslovanju gospodarskih družb. Zagotavljanje nemotenega poslovanja družbe, ugleda v javnosti, nedotakljivosti premoženja ter zagotavljanje varnosti in zdravja pri delu, je v marsičem odvisno od opredeljenih odgovornosti (odgovornega dela!) korporativno varnostnega menedžerja.

Osnove pravne odgovornosti

KVM je lahko član uprave gospodarske družbe oz. član organov vodenja družbe (njen svetovalec ali pa zaseda drugo vodilno oz. vodstveno funkcijo v gospodarski družbi). To pomeni, da je njegova odgovornost neprimerno večja od odgovornosti »običajnega« delavca v gospodarski družbi. V nadaljevanju bom zaradi boljšega razumevanja predstavil osnove civilne odgovornosti[1], ki izhajajo iz našega pravnega reda, saj le te zadevajo tudi korporativno varnostnega menedžerja.[2]

Skladno s 1. odstavkom 263. člena Zakona o gospodarskih družbah (Uradni list RS, št. 65/09 – uradno prečiščeno besedilo, 33/11, 91/11, 32/12, 57/12, 44/14 – odl. US in 82/13, v nadaljevanju ZGD-1), član organa vodenja ali nadzora mora pri opravljanju svojih nalog **ravnati v dobro družbe s skrbnostjo vestnega in poštenega gospodarstvenika in varovati poslovno skrivnost družbe**.

Člani organov vodenja ali nadzora so po imenovanju in prevzemu funkcije v t.i. korporacijsko pravnem razmerju z družbo, ki je urejeno v ZGD-1. Gre za profesionalne osebe, ki na trgu opravljajo svoje storitve za plačilo ter se zanje predpostavlja, da imajo strokovna znanja, ki so potrebna za pravilno opravljanje storitev. Ta ravnanja se zato presojajo po abstraktnih merilih stroke, za področja pri katerih so strokovna znanja potrebna za opravljanje teh storitev. Gre načeloma za objektivno merilo strokovnosti, vendar pa je odgovornost članov organov vodenja ali nadzora kljub temu krivdna (subjektivna).[3]

*avtor je član Slovenskega združenja korporativne varnosti



Pri tej odgovornosti gre za kriterij profesionalne skrbnosti, ki jo določa Obligacijski zakonik v 6. členu: »*udeleženci v obligacijskem razmerju morajo pri izpolnjevanju obveznosti iz svoje poklicne dejavnosti ravnati z večjo skrbnostjo, po pravilih stroke in po običajih (skrbnost dobrega strokovnjaka)*«. Tu gre za predpostavljeno krivdno odškodninsko odgovornost (skrbnost dobrega strokovnjaka) z *obrnjenim dokaznim bremenom*.

Odškodninska odgovornost je obligacijsko razmerje, v katerem je ena stranka zavezana povrniti povzročeno škodo drugi stranki, ta pa je upravičena zahtevati povrnitev. Odškodninska odgovornost članov organov vodenja ali nadzora nastane v razmerju do delniške družbe, ki je tudi pravno legitimirana za vložitev tožbe zoper odgovorne člane organov vodenja ali nadzora. Za odškodninsko odgovornost veljajo splošne predpostavke za nastanek odškodninske obveznosti po civilnopravnih predpisih (nastop določenih pravnih dejstev), in sicer:[4]

- protipravnost kot škodljivo dejstvo, ki ga stori član organa vodenja ali nadzora s tem, ko krši svoje dolžnosti (zakonsko in statutarne določene pristojnost itd.) oziroma jih ne opravlja s skrbnostjo vestnega in poštenega gospodarstvenika, pri čemer nastane škoda;
- nastanek nedopustne škode kot posledica kršitve dolžnosti; če so bile dolžnosti kršene, vendar škoda še ni nastala, odškodninske obveznosti ni;
- vzročna zveza med škodljivim dejstvom in nedopustno škodo, ki se presoja po načelu adekvatne vzročnosti;
- odškodninska odgovornost – obrnjeno dokazno breme.

Kot škodljivo dejstvo se šteje vsako dejanje ali opustitev, ki pomeni kršitev obveznosti članov organa vodenja ali nadzora (protipravnost ravnanja, kot na primer prepoved vračila in obrestovanja vložkov, prepoved vpisa lastnih delnic, nespoštovanje standarda dobrega gospodarstvenika ipd.). To so lahko v praksi posamezni posli in dejanja, ki jih člani organov vodenja ali nadzora storijo v nasprotju z zakoni, statutom, akti družbe, predpisi ali ustaljeno poslovno prakso ter po drugi strani opustitve dolžnih ravnanj (skrbnost vestnega in poštenega gospodarstvenika). Nekatere zakonodaje (na primer nemški AktG) natančno določajo dejanja članov organa vodenja, ki pomenijo povzročitev škode družbi. Škodljivo dejstvo mora v morebitnem sporu dokazati družba oziroma oškodovanec.

KVM je dejansko dolžan in odgovoren uresničevati naslednji moto: *»Korporativna varnost ni nekaj, kar imamo v podjetju, temveč je nekaj, kar dejansko počnemo.«*

Skrbnost vestnega in poštenega gospodarstvenika

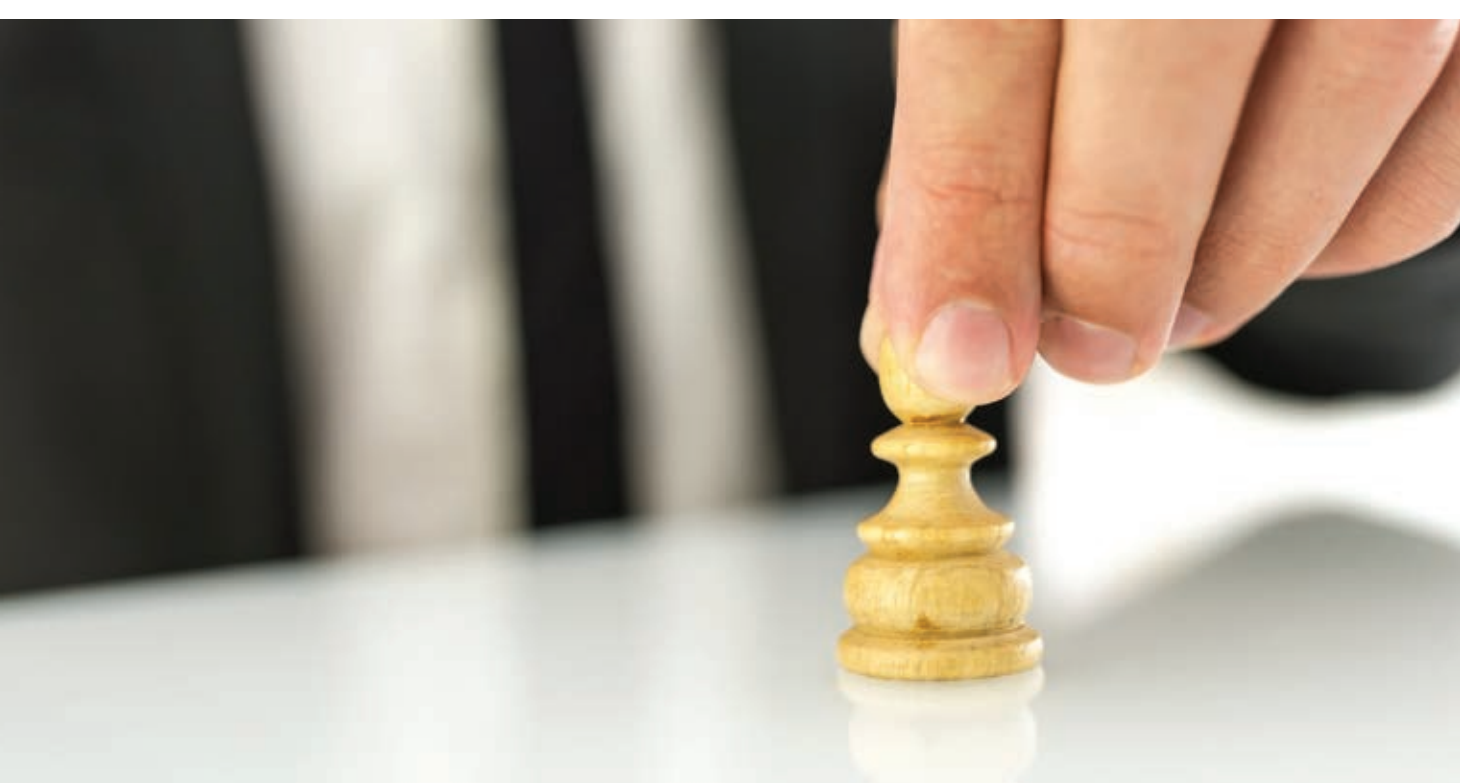
Standard skrbnosti (vesten in pošten gospodarstvenik), ki velja za člane organov vodenja in nadzora, je treba razlagati v okviru načel in pravil obligacijskega prava. Na splošno v primerjalnem pravu lahko ugotovimo, da se od članov organov vodenja zahteva, da svoje obveznosti izpolnjujejo pošteno in s posebno skrbnostjo. Opustitev navedene skrbnosti pri izpolnjevanju obveznosti povzroči nastanek odškodninske odgovornosti. Temeljna predpostavka je, da gre za profesionalno delo in da so člani organov vodenja in nadzora strokovno usposobljeni za opravljanje funkcije. Pri tem se upoštevata povprečno strokovno znanje in povprečna skrb članov organov vodenja. Na odgovornost posameznega člana vpliva delitev dela med člani in odgovornost za posamezna področja. Če so določeni člani imenovani v delovno skupino, ki naj pripravi določene predloge, je njihova odgovornost bistveno večja od odgovornosti članov, ki sprejmejo sklep na podlagi predloženega gradiva. Ti so odgovorni, če niso dovolj skrbno preučili predlogov delovne skupine. Odškodninska odgovornost članov se ne spreminja po razrešnici, ki jo dobijo po sprejetju letnega poslovnega poročila. Odpoved odškodninskim zahtevkom zoper člana vodenja ni mogoča pred iztekom treh let. Tudi statutarna omejitev odgovornosti članov vodenja ni dovoljena.

Konkretno o odgovornostih (dolžnostih) korporativno varnostnega menedžerja

Korporativno varnostni menedžer je pomemben in enakopraven partner pri vodenju in upravljanju gospodarske družbe. Njegova ključna odgovornost je skrbeti za poslovno oz. korporativno varnost, vzpostaviti in vzdrževati učinkovito sodelovanje z vsemi ključnimi deležniki v gospodarski družbi, predvsem pa s posameznimi direktorji (menedžerji), z namenom zaščite poslovanja in pravočasne prepoznave in obvladovanja poslovnih tveganj. Osnova te odgovornosti korporativno varnostnega menedžerja je v naslednjem:

- zagotavljati tesno sodelovanje vseh osnovnih in podpornih poslovnih procesov (funkcij) v podjetju, z namenom zagotavljanja varnosti premoženja, reda, zaščite in neprekinjenega poslovanja (**Leadership**);
- prepričevati kolege, sodelavce znotraj podjetja, da je zagotavljanje varnosti sestavni del opravljanja njihovih del in nalog in vsakodnevnih odločitev in ne zgolj še eno delovno področje (**Corporate culture**);
- upravljanje sprememb v podjetju na podlagi graditve zaupanja, varnostne kulture, močne socialne mreže in medsebojne povezanosti ter učenja in ne samo izvajanje korporativne varnosti kot podporni poslovni proces (**Change management**);
- upravljanje tveganj: izobraževanje s tega področja, vodenje delovnih skupin, načrtovanje ukrepov, itn. (**Risk management**);
- soodgovornost za strateško odločanje in upravljanje (**Management**);
- izvajanje dolžnostnega nadzorstva nad delom v podjetju oz. potekom osnovnih poslovnih procesov (**Comand & Control**).

KVM je dejansko dolžan in odgovoren uresničevati naslednji moto: *»Korporativna varnost ni nekaj, kar imamo v podjetju, temveč je nekaj, kar dejansko počnemo.«*



KVM ima pravico in dolžnost (je odgovoren!) v podjetju skrbeti za vzpostavitev in ohranjanje t.i. varnostne arhitekture – tehničnega, organizacijskega in funkcionalnega sistema korporativne varnosti, ki ga sestavljajo:

- varnostna strategija in standardi;
- varnostni podsistemi: CCTV, fizično, tehnično, mehansko, informacijsko varovanje, pristopna kontrola;
- informacijski sistem;
- sistem dokumentiranja in arhiviranja;
- ustvarjanje varnostne kulture;
- integriteta;
- spoštovanje domačega in mednarodnega pravnega reda ter predpisov podjetja (**compliance**);
- konkretni varnostni ukrepi.

Zgoraj navedeno pomeni, da je potrebno zagotavljati poslovno varnost v gospodarskih družbah predvsem zaradi vse večjih zahtev domače in mednarodne zakonodaje in pričakovanj deležnikov po zaščiti premoženja in ustvarjanju dobička podjetja (**compliance**):

- delovna razmerja: ZDR, Kolektivne pogodbe,
- varnost: ZVZD, AEO (Carina), C-TPAT (Carina), OHSAS 18001, Letalska varnost,
- požarna varnost: Zakon o požarni varnosti in predpisi izdani na njegovi podlagi,
- varstvo osebnih podatkov in informacijska varnost: ZVOP, ISO 27001, ...
- neprekinjeno poslovanje: Poslovni načrti podjetja, načrti neprekinjenega poslovanja,
- zaščita delničarjev: Sarbames Oxley Act, zahteve lastnikov, skupščine delničarjev, ...
- svetovna carinska organizacija - World Customs Organizations & US Custmos and Border Protection,
- Evropska komisija: AEO regulated requirements (zahteve za pridobitev statusa Pooblaščenega gospodarskega subjekta).

Posledice opustitve skrbi za varnost (**non-compliance**) se izražajo v naslednjem:

- kazenske ovadbe in zaporne kazni;
- postopki o prekršku in globe;
- pogodbene kazni in odpovedi pogodb o poslovnem sodelovanju;
- izguba ugleda družbe ali načet ugled družbe;
- izguba tržnega deleža;
- odliv ključnega kadra iz podjetja;
- odpovedi delovnih razmerij s strani delavcev;
- zastoji pri poslovanju podjetja;
- nesreče pri delu in bolniške odsotnosti;
- drugo.

Odgovornost korporativno varnostnega menedžerja pomeni dodano vrednost v podjetju

Narava dela korporativno varnostnega menedžerja in vse njegove odgovornosti v podjetju, pomenijo v bistvu osnovno garancijo za zagotavljanje skladnosti poslovanja (compliance) podjetja. Dejstvo je, da korporativno varnostni menedžer s svojim delom nedvomno pripomore k ohranjanju in zviševanju vrednosti premoženja, ustvarjanju dobička za lastnike, izkazovanju integritete, izkazovanju družbene odgovornosti, pospeševanju prodaje izdelkov ali storitev in s tem ustvarjanju dobička, nemotenem delovanju vseh osnovnih in podpornih procesov v družbi ter večanju tržnega deleža in ugledu podjetja



Narava dela korporativno varnostnega menedžerja in vse njegove odgovornosti v podjetju, pomenijo v bistvu osnovno garancijo za zagotavljanje skladnosti poslovanja (compliance) podjetja.

(zaupanje javnosti, zaposlenih in drugih deležnikov). Vse navedene odgovornosti v bistvu predstavljajo *ustvarjanje dodane vrednosti podjetja* (zagotavljanje varnosti se lahko prodaja kot »Unique Selling Point«, obračuna se lahko kot dodatna marža!).

[1] Zaradi omejenosti prostora za predstavitev prispevka, sem namenoma izpustil opredeljevanje osnov kazenske odgovornosti zaradi storjenega kaznivega dejanja.

[2] Naziv korporativni varnosti menedžer pomeni osebo, ki je v gospodarski družbi dolžna in upravičena skrbeti za stanje korporativne oz. poslovne varnosti. Ta oseba ima seveda lahko tudi drugačen naziv, kot na primer vodja varnostne politike, direktor sektorja za korporativno / poslovno varnost, varnostni menedžer, varnostni svetovalec, svetovalec uprave za varnost, ipd.

[3] Povzeto po: Dr. Dušan Jovanovič, Ekonomsko-poslovna fakulteta

[4] Povzeto po: Maja Rečnik, Skrbnost in odgovornost članov organov vodenja in nadzora, Podjetje in delo, 4. Marec 2011. ■

Avtor: GEA College / Fakulteta za podjetništvo*

INTERVJU
doc. dr. Denis Čaleta
Inštitut za korporativne varnostne študije, Ljubljana

ZADOVOLJNI ZAPOSLENI – VARNO PODJETJE

Cilj magistrskega programa Management korporativne varnosti je izobraževanje in usposabljanje podjetnikov in menedžerjev za obvladovanje poslovno-varnostnih mehanizmov v gospodarstvu, industriji, državnih institucijah in civilni družbi.

Podiplomski študij korporativne varnosti je novost v Sloveniji in v širši regiji, razmere na trgu pa kar kličejo po dobrih korporativno varnostnih strokovnjakih.

Okolje v katerem živimo, že dolgo ni več idilična oaza, varna pred mednarodnimi grožnjami, ampak je iz dneva v dan spreminjajoča se „zbirka groženj“, ki jih morajo podjetja znati predvidevati in se jim izogibati. Tukaj nastopijo dobro izobraženi varnostni strokovnjaki, tako imenovani „corporate security managerji“, ki jim na podiplomskem študiju letos prvič odpira vrata Fakulteta za podjetništvo GeaCollege. O varnostnih vprašanjih, ki se jih podjetja še premalo zavedajo, smo govorili z vrhunskim slovenskim strokovnjakom na tem področju, dr. Denisom Čaleto, predsednikom sveta Inštituta za korporativne varnostne študije ICS, predsednikom Slovenskega združenja korporativne varnosti in prihodnjim predavateljem na fakulteti za podjetništvo GeaCollege.

Cilj magistrskega programa Management korporativne varnosti je izobraževanje in usposabljanje podjetnikov in menedžerjev za obvladovanje poslovno-varnostnih mehanizmov v gospodarstvu, industriji, državnih institucijah in civilni družbi.

> Iluzija, da živimo v družbi, ki je varna in sama sebi namen, se je že zdavnaj podrla. Živimo v povezanem svetu, kjer so grožnje, ki jih čuti mednarodno okolje, zelo prisotne tudi pri nas.

Kaj pomeni pojem korporativna varnost?

Korporativna varnost je v najširšem pomenu besede dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju. Kot taka predstavlja eno od osnovnih funkcij za delovanje podjetja in se za njegovo učinkovito delovanje nujno izvaja v tesnem sodelovanju z vsemi ključnimi funkcijami v podjetju. Procesi zagotavljanja korporativne varnosti so nedeljiva celota krovnega modela upravljanja korporacij in se izraža skozi korporativno upravljanje in korporativno družbeno odgovornost.

Eden od pomembnih notranjih dejavnikov tveganja so zaposleni v podjetjih. Zakaj predstavljajo tako veliko tveganje?

Zaposleni so zaradi dinamike in hitrega menjavanja služb vedno manj lojalni do delodajalcev, ker je proces zagotavljanja varnostne kulture in zavedanja pripadnosti podjetja daljši. Zelo težko je zaposlene vključiti v podjetje, tako da so lojalni in varnostno dovolj ozaveščeni. Varnost je predvsem pri zaposlenih najbolj izpostavljen notranji dejavnik, ki je povezan s kriminalnimi dejanji, odtekanjem ključnih informacij, poslovnih skrivnosti in patentov. Iluzija, da živimo v družbi, ki je varna in sama sebi namen, se je že zdavnaj podrla. Živimo v povezanem svetu, kjer so grožnje, ki jih čuti mednarodno okolje, zelo prisotne tudi pri nas.

Kaj se bolje obnese za zagotavljanje varnosti v podjetjih: da podjetja delajo na povečevanju občutka pripadnosti zaposlenih ali da krepijo varnostne ukrepe?

Nujna je kombinacija obojega. Zadovoljni zaposleni so tudi lojalni zaposleni. Na drugi strani pa morajo biti vzpostavljeni primerni mehanizmi nadzora. Novo zaposleni mora poznati organizacijsko in

*Vsebina objavljena tudi na spletnem portalu PLANET SIOL.NET.



varnostno kulturo v podjetju. Če temu ne namenjamo dovolj pozornosti, zaposleni ne ve, kaj sme in česa ne sme početi v organizaciji. Tega se strateška vodstva podjetij v Sloveniji premalo zavedajo.

Ali uprava lahko naredi več škode za varnost v podjetju kot zaposleni?

Situacija je zelo podobna piramidi. Uprava operira s ključnimi informacijami, ki so tudi po vrednosti v primeru odtekanja najnevarnejše. Veriga je tako močna, kot je njen najšibkejši člen. Vsak zaposleni v organizaciji je zelo pomemben, uprava pa mora s svojim zgledom in integriteto voditi zaposlene.

Kaj pa se lahko zgodi, če podjetje propade zaradi neupoštevanja varnostnih tveganj ali groženj?

V konkurenčni tekmi na globalnem trgu so uspešna tista podjetja, ki so se sposobna čim hitreje prilagoditi novim situacijam. Če strateško vodstvo podjetja zanemari obvladovanje varnostnih in drugih s tem povezanih tveganj, podjetje izpostavi veliki nevarnosti, da bo začelo močno zaostajati, kar v končni posledici pomeni tudi izgubo vrednosti delnic podjetja, izgubo delovnih mest, opustitev proizvodnih programov in nenazadnje propad podjetja. Zato morajo lastniki podjetij zahtevati, da se z njihovim premoženjem ustrezno upravlja, da so naložbe varne in nemoteno delujejo ter prinašajo povečanje vrednosti. Sicer bodo lastniki zahtevali odgovornost uprav, ki ne bo samo odškodninska. Uprave so v določenih segmentih tudi kazensko odgovorne zaradi neupoštevanja predpisanih varnostnih zahtev.

Če strateško vodstvo podjetja zanemari obvladovanje varnostnih in drugih s tem povezanih tveganj, podjetje izpostavi veliki nevarnosti, da bo začelo močno zaostajati, kar v končni posledici pomeni tudi izgubo vrednosti delnic podjetja, izgubo delovnih mest, opustitev proizvodnih programov in nenazadnje propad podjetja.

Največji izziv za zagotavljanje varnosti v podjetjih je verjetno to, da se vrsta groženj stalno spreminja in da se poslovno okolje vedno spreminja, s tem se spreminja tudi način, kako delamo. Kako so slovenska podjetja pripravljena na stalne spremembe in kakšna je pri tem vloga strokovnjakov za varnost?

V Inštitutu za korporativne varnostne študije vsako leto izvajamo raziskavo korporativnega varnostnega managementa. Rezultati razkrivajo, da se strate-

ški management v slovenskih podjetjih, predvsem v tistih, ki nimajo jasnega lastnika, ne zaveda teh težav. Tveganj nikoli ne moremo popolnoma obvladati. Treba se je približati neki stopnji optimalnosti, na katero imajo velik vpliv resursi in znanje, ki jih imamo na voljo, da glavni poslovni proces lahko teče nemoteno. Korporativna varnost podpira in blaži tveganja na še sprejemljivo raven.

Kaj so delovne naloge strokovnjaka za varnost, t. i. »corporate security managerja«?

Korporativni varnostni manager krovno skrbi za fizično in tehnično varnost, varnost ključnih informacij, varnost zaposlenih, neprekinjenost delovanja podjetja in drugih dejavnosti, ki so posredno in neposredno povezane z obvladovanjem tveganj. **Korporativni varnostni manager je podaljšana roka strateškega managementa.** V Sloveniji je težava, ker se korporativni varnostni managment pojavlja na peti ali šesti ravni odločanja, zato varnostni procesi in težave težko pridejo na mizo reševanja strateškega managementa. Če podjetja glavne procese načrtujejo, ne da bi upoštevala tudi varnost, je sistem neustrezen. Do zdaj v Sloveniji in širši regiji ni bilo izobraževalnega programa, ki bi korporativnim varnostnim managerjem dal dovolj kakovostna in široka znanja, da bi lahko primerno obvladovali vse izzive, s katerimi se spopadajo v globalnem dinamičnem varnostnem okolju.

GeaCollege letos prvo leto vpisuje na podiplomski program Management korporativne varnosti. Kakšna znanja in veščine bo osvojil magister tega programa oziroma korporativno varnostni manager?

Vsekakor je to velik korak naprej za profesijo korporativne varnosti. Vsaka profesija, zdravniška ali pravniška, lahko učinkovito deluje, če ima v ozadju učinkovit izobraževalni sistem, ki trgu stalno ponuja dovolj kakovostnih kadrov. Program korporativne varnosti na Fakulteti za podjetništvo GeaCollege je velik korak naprej v tej smeri. To je program, ki je redek tudi v širšem mednarodnem okolju, saj združuje multidisciplinarna znanja s pravnega, varnostnega in poslovnega področja ter z drugih področij. Najboljšim študentom na tem programu bomo omogočili neposredno prakso v mednarodnih korporacijah, tako da jih bomo čim več poslali v tujino, kjer je ta dejavnost mnogo bolj razvita kot pri nas. Že ob študiju bodo tako lahko preverili uporabnost znanj, ki so jih pridobili, in jih primerjali v realnem okolju.

Kakšna je potreba po tovrstnem kadru v slovenskih podjetjih?

Izredno velika. Vprašanje pa je, ali se podjetja zavedajo, da te kadre potrebujejo. Ob akreditaciji programa smo naredili podrobno analizo, ki je pokazala, da so potrebe po tem kadru izredno velike. V Sloveniji imamo kar nekaj organizacij, ki obvladujejo kritično infrastrukturo, naj

Korporativni varnostni manager je podaljšana roka strateškega managementa.





navedemo samo nekatere: Aerodrom Ljubljana, Telekom Slovenije, sektor proizvodnje in prenosa električne energije ter drugih energentov, del cestne in železniške infrastrukture in še bi lahko naštevali. Že zaradi pomembnosti te infrastrukture, ki mora neprekinjeno delovati, da naša družba lahko normalno deluje, te organizacije potrebujejo varnostne strokovnjake. V organizacijah, ki so vpete v mednarodno okolje, so varnostni strokovnjaki ključni, saj velja: „Sodelujem s teboj, če sem prepričan, da so informacije, ki jih bom predajal v tem poslu, pri tebi varne."

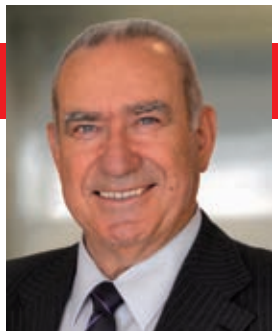
Ali lahko napoveste, kakšen delež diplomantov lahko računa na zaposlitev?

Preostale fakultete, ki se ukvarjajo z varnostjo in so usmerjene predvsem na področje policije, vojske in varnostno-obveščevalnih služb, imajo skoraj nično zaposljivost, kajti državna uprava je popolnoma prenehala zaposlovati. Zato so vsi diplomanti, ki prihajajo s teh fakultet, na žalost nezaposljivi. Želja in usmerjenost našega programa je poseči v tržno nišo poslovnega področja, povezanega s korporativno varnostjo, kjer teh profilov do zdaj ni nihče izobraževal. Ob pregledu mednarodnih razpisov vidimo, da je ogromno povpraševanja po korporativnih varnostnih strokovnjakih. Znanja, ki jih bodo pridobili na našem programu, bodo dovolj konkurenčna, da bo zaposljivost iz tega programa dovolj velika, da bo prihodnjim kandidatom dala signal, da je to tisto področje, v katerega se izplača usmerjati nadaljnje izobraževanje.

Kaj bo najbolj močno orožje diplomantov programa Management korporativne varnosti?

Program je sestavljen iz obveznega okvira predmetov, ki diplomantu dajejo znanja s pravnega, varnostnega in poslovnega področja. Korporativni varnostni manager mora razumeti poslovni proces in obvladati ustrezno upravljanje z varnostnimi tveganji. S svojimi aktivnostmi mora ustrezno podpirati ta poslovni proces. Ključno je zavedanje, da se poslovni procesi ne morejo prilagajati njemu in njegovi varnostni funkciji. Naš diplomant bo znal varnostni proces vključiti v vse segmente poslovanja. Študent se bo v nadaljevanju študija z izbirnimi predmeti lahko osredotočil na različna področja, ki so povezana z aktualnimi grožnjami in bodo v eni smeri bolj osredotočena na podjetniško okolje,v drugi smeri pa v večje organizacijske sisteme, ki jih predstavljajo podjetja, ki obvladujejo kritično infrastrukturo ali večja korporacijska okolja. ■

Avtor: doc. dr. Milan Vršec / Inštitut za korporativne varnostne študije



VODSTVENI NADZOR V PROCESU UPRAVLJANJA KORPORATIVNE VARNOSTI

Morda je pravi čas, da v okviru tematik, ki jih obravnava revija Korporativna varnost spregovorimo tudi o vodstvenem nadzoru kot pomembnem dejavniku v procesu upravljanja korporativne varnosti.

Da so nadzorni mehanizmi v naši državi prepoznavno neučinkoviti (več o tem Vršec 2014) ni treba posebej poudarjati. Ko pa govorimo o nadzornih mehanizmih na področju korporativne varnosti pa na osnovi spoznanj iz naših projektov ugotavljam, da pravega profesionalnega nadzora na vseh nivojih preprosto ni opaziti. To velja zlasti za strateško raven, kjer govorimo o vodstvenem nadzoru, ki je v domeni lastnikov, upravljavcev in nadzornikov, v bistvu pa ena od glavnih nalog strateškega varnostnega managementa. V tem kontekstu se je treba dotakniti tudi nadzora na področju varnostnih storitev, ki je v mnogih gospodarskih in drugih družbah pogodbeno vpeto v upravljanje korporativne varnosti. Tudi tovrstni vodstveni in operativni nadzor se ne moreta pohvaliti z učinkovitostjo. Tega se na žalost premalo zavedajo nadzorni mehanizmi organov za notranje zadeve, vodstev varnostnih podjetij in Zbornica za razvoj slovenskega zasebnega varovanja. Problem je treba iskati tudi v ugotovitvi, da varnostni management – zlasti na strateški ravni – preprosto nima kje dobiti ustreznega znanja in kompetenc za izvajanje svojega poslanstva. Fakulteta za varnostne vede, ki bi morda bila najbolj poklicana za nudenje ustreznega znanja se je odrekla tovrstnih predmetnih področij. Torej, bomo videli kako se bo na Fakulteti za podjetništvo v prihodnosti odrezal magistrski program Management korporativne varnosti.

IZHODIŠČE: Pomembno je vzpostaviti sistem korporativne varnosti v kritični infrastrukturi in multinacionalkah

Že dolgo je znano, da je kritična infrastruktura vse tisto kar je neizogibno potrebno za funkcioniranje države ter za zagotavljanje potreb gospodarstva, civilne družbe in prebivalstva. Zato se osredotočam na korporativno varnost in na vodstveni nadzor v kritični infrastrukturi in v multinacionalkah (več o tem Lewis 2014 in Vršec 2012), ki v večjem obsegu poslujejo tudi na tujih trgih. Nacionalno kritično infrastrukturo sestavljajo: energetika (ELES, NEK, Petrol, Geoplin), transport (Aerodrom, Ljubljana in Maribor, Slovenske železnice, Luka Koper, DARS), kmetijstvo, prehrambena industrija, voda in vodovodni sistemi, javno zdravstvo (Klinični center Ljubljana in Maribor in druge zdravstvene ustanove), zaščita in reševanje, obrambna industrija, intervencijske službe (policija, gasilske službe, urgenca, reševalne službe), telekomunikacije (Telekom in drugi), bančništvo (NLB in druge), kemikalije in nevarne snovi, poštne storitve (Pošta Slovenije), logistika (Intereuropa in drugi), jezovi, pregrade in nasipi, skladišča, deponije in ravnanje z radioaktivnimi snovmi, pomembne poslovne zgradbe, državne institucije. Energetika in transport sta opredeljeni kot evropska kritična infrastruktura (Direktiva Sveta (EU, št. 114/2008 in slovenska uredba, Ur. l. RS, št. 25/2011).



*avtor je član Slovenskega združenja korporativne varnosti

Vsaka gospodarska družba v kritični infrastrukturi in vsaka multinacionalka bi morala imeti vsaj enega korporativnega varnostnega managerja, ki bi na strateški ravni korporativnega upravljanja znal in zmogel vzpostaviti sistem in proces upravljanja korporativne varnosti.

Poleg kritične infrastrukture so pomembne tudi multinacionalke med katerimi so tudi take, ki so sestavni del kritične infrastrukture. Najbolj internacionalizirane multinacionalke, torej tiste, ki največ poslujejo s tujino so: Splošna plovba Portorož, Gorenje, Krka, Iskra avtoelektrika, Trimo, ETI, Impol, Alpina, Perutnina, Lisca, Kovinotrade, Iskraemeco, Hidria, Mercator, Unior, Kolektor, Petrol, Telekom, Zavarovalnica Triglav in druge.

Vse bolj je jasno in prepoznavno, da je kritična infrastruktura pod udarom vse večje ogroženosti iz narave, kriminalne in teroristične ogroženosti ter drugih vrst ogroženosti. To bi moralo državo, lastnike in upravljavce družb vzpodbuditi, da se bolj kot doslej posvetijo vzpostavljanju učinkovitejših varnostnih mehanizmov v kritični infrastrukturi in v multinacionalkah tako z vidika regulative, varnostne politike in ustvarjanju materialnih pogojev delovanja.

Vsaka gospodarska družba v kritični infrastrukturi in vsaka multinacionalka bi morala imeti vsaj enega korporativnega varnostnega managerja, ki bi na strateški ravni korporativnega upravljanja znal in zmogel vzpostaviti sistem in proces upravljanja korporativne varnosti.

Koncept integriranega vodstvenega nadzora

Tisti, ki se ukvarjajo z uvajanjem in upravljanjem standardov kakovosti in varnostnih standardov po ISO 9000, ISO 31000, ISO 27000, ISO 22000, ISO 14000, OHSAS 18001 in drugimi vedo, da je vodstveni nadzor že vtkan v strukturo teh standardov. Torej je že solidna osnova za vodstveni nadzor v procesih upravljanja korporativne varnosti, če ima gospodarska in druga družba uvedene nakazane standarde. Za integriran vodstveni nadzor v kritični infrastrukturi in v multinacionalkah pa je treba zagotoviti še naslednje:

- formalnopravno in kadrovsko vzpostaviti management korporativne varnosti, ki bo sposoben in motiviran obvladovati stroko varovanja, varnostna tveganja in stroške varovanja; in s tem prispevati k izboljšanju poslovnih rezultatov,
- pripraviti, sprejeti in implementirati krovno varnostno politiko in varnostno strategijo (glej Vršec 2012),
- naročiti varnostni elaborat in načrt varovanja ljudi in premoženja pri zunanji neodvisni instituciji in ga implementirati v integralni varnostni sistem in proces upravljanja korporativne varnosti (glej Vršec 2014),
- z uvedbo varnostnih standardov in metod ocenjevanja tveganj vzpostaviti sistem upravljanja varnostnih tveganj (glej Vidic 2012 in Vršec 2012),
- vzpostaviti sinergijo med posameznimi strokovnimi področji varnosti, kot so: varnost in zdravje pri delu, varstvo pred naravnimi in drugimi nesrečami-zaščita in reševanje, varstvo okolja, varstvo pred požari, varstvo osebnih in tajnih podatkov, informacijska varnost, varovanje poslovnih skrivnosti, idr. (glej Vršec 2014),



- izkoristiti vse možnosti zgodnjega opozorilnega sistema kot so anonimne prijave o napakah, škodoželjnih nakanah, kriminalnih ravnanjih, javni in interni alarmni sistem, notranja kontrola in revizija ipd.,
- v planu neprekinjenega poslovanja in v kriznem načrtu (po konceptu standarda BS 25999) opredeliti tudi vodstveni nadzor pri upravljanju korporativne varnosti,
- za celovito obvladovanje tveganj si mora gospodarska in druga družba ustvariti ustrezen zavarovalni portfelj glede zavarovanja premoženja, ljudi in odgovornosti.

Temeljno načelo integriranega vodstvenega nadzora v procesih upravljanja korporativne varnosti je: »Preprečevanje škod in izgub« (Loss Prevention – glej Purpura 2013). To je izredno pomembno načelo korporativnega upravljanja, ki vsebuje tudi obvladovanje kriminalnih in drugih škodljivih ravnanj; in je vneseno celo v dokumente OECD, ki se nanašajo na korporativno upravljanje. Če pogledamo v AMAZON.com books najdemo kar nekaj del o vodstvenem nadzoru (glej npr. Davies 2007), ki dokaj celovito obravnavajo to področje managementa.

Vloga lastnikov in upravljavcev

Lastniki in upravljavci (uprave, direktorji) bi si morali vzpostaviti učinkovite nadzorne mehanizme preko nadzornih, notranje kontrolnih in notranje revizorskih teles in preko zunanjih nadzornih institucij. Vse bi moralo delovati preventivno in represivno v skladu z zakonodajo, standardi, poslovnimi in etičnimi načeli ter dobro prakso. Poglavitni je torej interes lastnikov in upravljavcev kot formalnih dejavnikov korporativnega upravljanja. Če je interes, da se gospodarska ali druga družba razvija v pozitivno smer je verjetnost, da bo deloval tudi nadzor, v nasprotnem pa so nadzorni mehanizmi – od zgoraj navzdol - potisnjeni v ozadje. V taki situaciji ni prostora za integriran vodstveni nadzor v procesih korporativnega upravljanja. Škarje in platno korporativnega upravljanja imajo torej lastniki in upravljavci, ki si vzpostavijo razvojno ali razdiralno (uničevalno) filozofijo upravljanja in vodenja. Če bi deloval management korporativne varnosti bi se zagotovo zmanjšal manevrski prostor za razdiralne filozofije.

Korporativni varnostni manager - predstavnik vodstva za korporativno varnost, v vlogi strateškega nadzornika

Jasno je, da korporativni varnostni manager deluje na strateški ravni korporativnega upravljanja. To je osnova, da lahko uveljavlja svoja stališča, predloge in rešitve in soodloča o zadevah korporativne varnosti in o zadevah, ki se neposredno ali posredno dotikajo upravljanja korporativne varnosti. Vendar pa morajo biti za tak status korporativnega varnostnega managerja izpolnjeni naslednji pogoji:

- **opredelitev statusa** v notranjih aktih gospodarske in druge družbe, kjer je navedeno, da je korporativni varnostni manager označen kot **predstavnik vodstva za korporativno varnost,** tako kot je denimo za področje vodenja sistema kakovosti,
- **jasna določitev kompetenc**, pristojnosti, pooblastil in odgovornosti v odločbi oziroma v pogodbi o zaposlitvi,
- **podpora** lastnikov, upravljavcev in nadzornikov pri pridobivanju avtoritete, integritete in spoštovanja pri zaposlenih, poslovnih partnerjih, pogodbenih izvajalcih in zunanjih nadzornih organih,
- **primerno plačilo** (plača), ki se meri po merilih vrednotenja upravljavcev, nadzornikov in vrhnjega managementa.

Če bi deloval management korporativne varnosti bi se zagotovo zmanjšal manevrski prostor za razdiralne filozofije.



Logično je sklepati, da so krizni časi priložnost za izboljšanje upravljanja korporativne varnosti na strateški ravni, kjer naj bi dobil svoje mesto tudi korporativni varnostni manager. Če bodo lastniki in upravljavci dojeli, da je integriran nadzor v procesih upravljanja korporativne varnosti tudi eden od poglavitnih dejavnikov uspešnega poslovanja, se zna zgoditi pozitivni premik vsaj v družbah kritične infrastrukture.

Nadzor nad pogodbenimi varnostnimi in drugimi storitvami

Glede na to, da veliko gospodarskih in drugih družb ter državnih in civilnih institucij na trgu varnostnih storitev pogodbeno najema fizične, tehnične svetovalne in druge storitve varovanja, je treba vzpostaviti vodstveni nadzor tudi na tem segmentu upravljanja korporativne varnosti. Gre za nadzor nad zakonitostjo, strokovnostjo, kakovostjo, organiziranostjo, sredstvi dela, sposobnostjo obvladovanja izrednih dogodkov in varnostnih tveganj, izvajanjem pogodbenih obveznosti, kadrovsko strukturo, plačami ter dokumentacijo dela in poslovanja pogodbeno angažiranega varnostnega podjetja. Govorimo torej o celovitem nadzoru, ki pokaže s kakšnim varnostnim podjetjem imamo opravka. Vodstveni nadzor je potemtakem sredstvo za odločanje o nadaljnjem sodelovanju naročnika z izvajalcem. Sistem nadzora nad zunanjimi izvajalci raznih oblik varovanja pravzaprav sestoji iz štirih vrst nadzora, in sicer:

- vodstvenega nadzora, ki je predmet tega sestavka,
- notranjega nadzora, ki ga izvaja pogodbeni izvajalec z varnostniki nadzorniki, varnostni menedžerji in odgovorno osebo (določeno v pogodbi) za izvajanje pogodbenih obveznosti pri naročniku,
- notranjega nadzora, ki ga izvaja naročnik z odgovorno osebo za fizično, tehnično in požarno varovanje,
- inšpekcijskega nadzora, ki ga po Zakonu o zasebnem varovanju izvaja Inšpektorat RS za notranje zadeve,
- policijskega nadzora, ki ga na podlagi Zakona o policiji ter Zakona o zasebnem varovanju izvaja Policija.

Notranji nadzor izvajalca zasebnega varovanja z licencami je opredeljen v 12. členu Zakona o zasebnem varovanju, ki se glasi: »Imetnik licence mora zagotavljati lasten ali pogodbeni nadzor nad opravljanjem nalog varnostnega osebja z varnostniki-nadzorniki in varnostnimi menedžerji, ki morajo biti strokovno usposobljeni za opravljanje nalog po programu, ki ga določi minister«. Posebni segment vodstvenega nadzora v procesu upravljanja korporativne varnosti je nadzor nad pogodbenimi storitvami na področju informacijske in komunikacijske varnosti, ki je – strokovno gledano – v domeni službe za informatiko in inženirja in/ali izvršnega direktorja za informacijsko varnost. Vloga korporativnega varnostnega managerja pri tem segmentu nadzora je zlasti tehtanje in ocenjevanje tveganj angažiranja zunanjih izvajalcev upravljanja z informacijsko varnostjo in informacijsko tehnologijo. Kajti premisliti je treba kdo in kako naj upravlja poslovno skrivnost, zaupne podatke in informacije ter intelektualno lastnino.

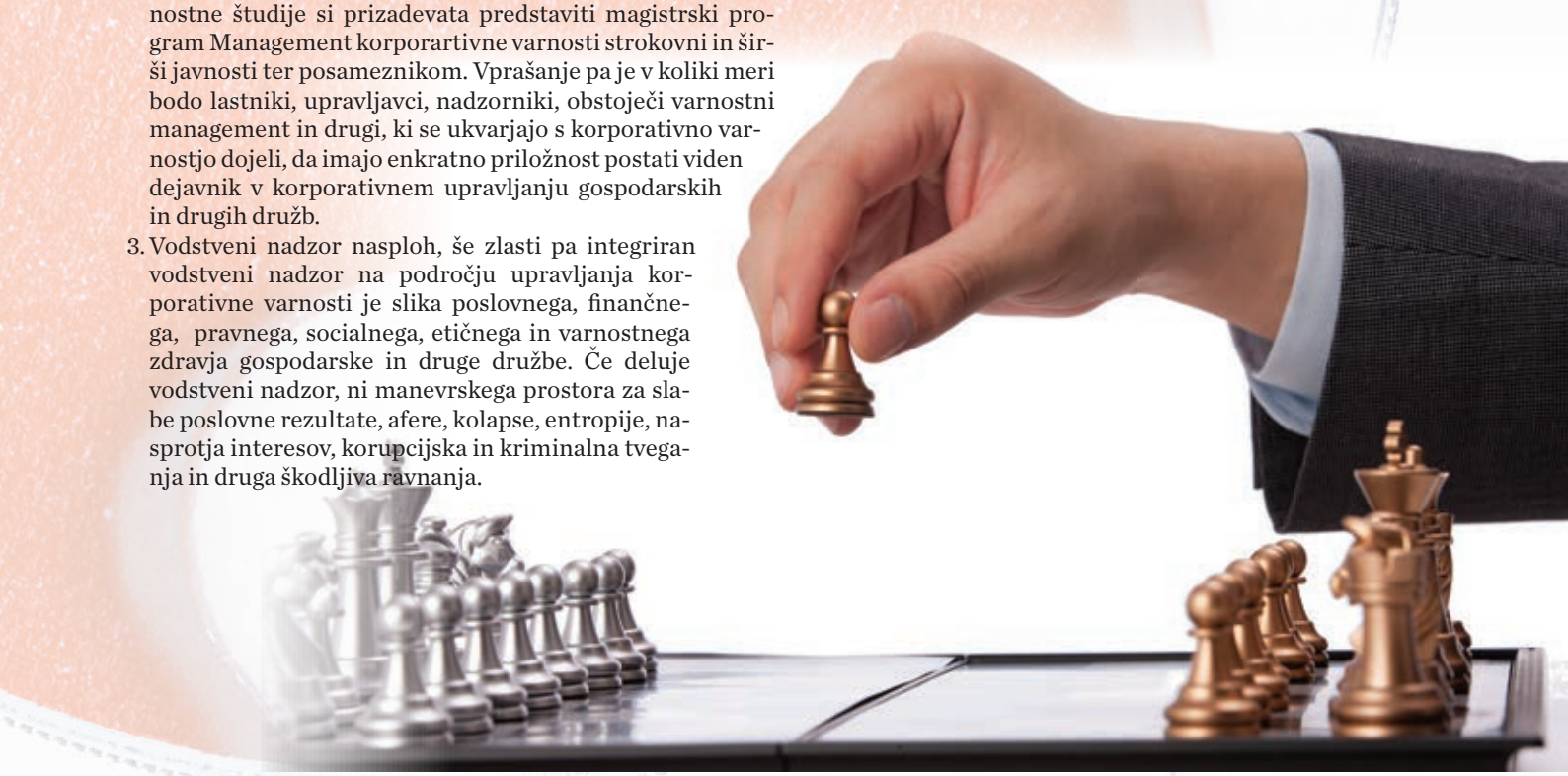
Zaključne misli

1. Za izvajanje integriranega vodstvenega nadzora v procesih upravljanja korporativne varnosti je potrebno ogromno interdisciplinarnega znanja, spoznaj in dognanj, ki jih je v sedanjem času možno pridobiti le v magistrskem programu Management korporativne varnosti.
2. Fakulteta za podjetništvo in Inštitut za korporativne varnostne študije si prizadevata predstaviti magistrski program Management korporartivne varnosti strokovni in širši javnosti ter posameznikom. Vprašanje pa je v koliki meri bodo lastniki, upravljavci, nadzorniki, obstoječi varnostni management in drugi, ki se ukvarjajo s korporativno varnostjo dojeli, da imajo enkratno priložnost postati viden dejavnik v korporativnem upravljanju gospodarskih in drugih družb.
3. Vodstveni nadzor nasploh, še zlasti pa integriran vodstveni nadzor na področju upravljanja korporativne varnosti je slika poslovnega, finančnega, pravnega, socialnega, etičnega in varnostnega zdravja gospodarske in druge družbe. Če deluje vodstveni nadzor, ni manevrskega prostora za slabe poslovne rezultate, afere, kolapse, entropije, nasprotja interesov, korupcijska in kriminalna tveganja in druga škodljiva ravnanja.

In končno: Glede na to, da je kritična infrastruktura (z multinacionalkami vred) poglavitni dejavnik obstoja, delovanja in razvoja države, gospodarstva in civilne družbe bi bilo skorajda nujno da se lastniki, upravljavci in nadzorniki družb, ki predstavljajo kritično infrastrukturo zamislijo o svoji vlogi na področju vodstvenega nadzora in o prodoru nove paradigme, ki se glasi: »Riba ne sme smrdeti, ampak dišati pri glavi«.

Viri

- Davies, S. J., Hertig, C.A. (2007). Security Supervision and Management. Butterworth-Heinemann. New York, London.
- Lewis, T. G. (2014). Critical Infrastructure Protection in Homeland Security. Wiley&Sons, Inc..New Jersey.
- Purpura, P. P. (2013): Security and Loss Prevention. An Introduction. Butterworth-Heinemann. New York, London.
- Vidic, J. (2012). Ravnanje s tveganji. Korporativna varnost, štev. 2/2012. Inštitut za korporativne varnostne študije. Ljubljana.
- Vršec, M. (2010). Izzivi varnostnih managerjev. Nacionalni posvet. Inštitut za korporativne varnostne študije. Ljubljana.
- Vršec, M. (2012). Varnostna politika kot krovni dokument upravljanja korporativne varnosti. Korporativna varnost, štev. 2/2012. Inštitut za korporativne varnostne študije. Ljubljana.
- Vršec, M. (2012). Upravljanje poslovnih, varnostnih in drugih tveganj v multinacionalnih gospodarskih družbah. Mednarodna konferenca 2012. Inštitut za korporativne varnostne študije. Ljubljana.
- Vršec, Mir. (2014). Državni (ne)nadzorni organi. Korporativna varnost, štev. 7/2014. Inštitut za korporativne varnostne študije. Ljubljana.
- Vršec, M. (2014) Strateško načrtovanje procesov korporativne varnosti. Korporativna varnost, štev. 6/2014. Inštitut za korporativne varnostne študije. Ljubljana.
- Vršec, M. (2014). Sinergija v upravljanju korporativne varnosti. Korporativna varnost, štev. 7/2014. Inštitut za korporativne varnostne študije. Ljubljana. ■



Slovensko združenje korporativne varnosti

Slovensko združenje korporativne varnosti združuje pravne in fizične osebe s področja korporativne varnosti in drugih povezanih področij. Skozi združenje člani organizirano uresničujejo osebne in poslovne interese na področju korporativne varnosti.



»Ab uno disce omnes (po enem spoznaj vse)«

»Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!«

Namen združenja je uresničevanje interesov članstva, ki so:

- združevanje znanja, izkušenj, interesov in razvojnih pogledov,
- pospeševanje razvoja izobraževanja in usposabljanja,
- razvoj mednarodno primerljivih korporativnih varnostnih standardov,
- izboljšanje kakovosti storitev na področju zagotavljanja korporativne varnosti,
- razvoj korporativnega varnostnega managementa,
- razvoj varnosti kot vrednote, ki izboljšuje pogoje dela in dviguje motivacijo.

Članstvo v združenju je prostovoljno. Združenje ima redne, korporacijske in častne člane.

Ugodnosti za člane združenja:

- brezplačna udeležba na rednih strokovnih srečanjih;
- popusti pri nakupu izdanih publikacij ICS, Ljubljana;
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS, Ljubljana;
- brezplačna naročnina na revijo Korporativna varnost;
- popusti pri oglaševanjih in postavitev logotipa na spletno stran ICS-Ljubljana
- popusti pri članarinah za strokovne člane, ki prihajajo iz vrst organizacij, katere so korporacijski člani združenja;

Članstvo v SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI vam olajša obvladovanje tveganj v vaših organizacijskih sredinah. **SKUPAJ SMO MOČNEJŠI!**

www.ics-institut.si

hse Holding Slovenske elektrarne d.o.o.
KONTROLA ZRAČNEGA PROMETA SLOVENIJE
MARIBORSKI VODOVOD
energetika ljubljana
LUKA KOPER Port of Koper
interblock LUXURY GAMING PRODUCTS
Republika Slovenija
REISSWOLF secret. service.
TelekomSlovenije
SIEMENS
MIŠKA 20 let FMC Group
Zanesljivo vsepovsod POŠTA SLOVENIJE
DARS
Nova KBM PRIPRAVLJENI NA JUTRI
univerzitetni klinični center ljubljana
gorenje Gorenje, d.d.
si·cert
INFORMACIJSKI POOBLAŠČENEC

Avtor: doc. dr. Denis Čaleta / Institut za korporativno varnostne študije –ICS, Ljubljana*



KOLUMNA
denis.caleta@ics-institut.si

KORPORATIVNA VARNOST – POTI IN STRANPOTI V SMERI PROFESIJE

V zadnjem obdobju smo v modernem varnostnem okolju priča dvema temeljnima dejavnikoma, ki pomembno vplivata na razvoj organizacij in njihovo uspešnost. Prva je dinamičnost varnostnega okolja, ki se nenehno spreminja in pred nas postavlja vedno nove oblike varnostnih tveganj. Te imajo na učinkovitost in neprekinjenost delovanja poslovnih procesov zelo pomemben vpliv. Drugi pomemben dejavnik pa je vsekakor zahtevno ekonomsko okolje, ki se v pomembnem delu rezultira skozi gospodarsko krizo in hudo konkurenčno tekmo med poslovnimi organizacijami. Poslovna filozofija je vedno bolj usmerjena v cilj z manj storiti več in bolj kvalitetno. Vplivu teh procesov pa se ne more ogniti niti korporativna varnost, ki ima v organizacijah pomembno vlogo blažitve tveganj za nemotenost njihovega delovanja. Če pogledamo samo nekaj trenutno najbolj izpostavljenih lahko vidimo, da na mednarodno okolje poslovanja najbolj vplivajo rusko-ukrajinski konflikt, ebola. Fenomen Islamske države kakor tudi tveganja, ki so že dalj časa prisotna in se v zadnjem obdobju še krepijo v svojem pomenu, kakor na primer nelojalna konkurenca in kraja intelektualne lastnine ter patentov, kibernetska tveganja, organizirani kriminal, ugrabitve zaposlenih in njihovih družinskih članov in še bi lahko naštevali. Če vse to pogledamo še skozi prizmo zmanjševanja stroškov in optimizacije in pritiskov s strani investitorjev lahko vidimo, da so strokovnjaki korporativne varnosti postavljeni pred resne dileme kako naprej v cilju učinkovitega zagotavljanja varnosti organizacije, njenih poslovnih procesov in zaposlenih. Ko govorimo o ugledu korporativne varnosti in njeni organizacijski vključenosti v poslovne procese je nedvomno največ odvisno ravno od strateškega korporativno varnostnega managementa v organizaciji. Znanje ni omejeno samo na ozko področje varnosti temveč se vedno bolj širi tudi na področja informatike, poslovnih ved, prava in ostalih področij, ki zagotavljajo, da profesija korporativne varnosti postaja multifunkcionalna in kot taka tudi ustrezno prepoznana v svojem okolju. S tem je seveda povezan tudi njen ugled, ki za seboj potegne tudi ustrezno umeščenost v organizacijsko-odločevalsko strukturo podjetij. Če korporativno varnostni managerji ne razumejo poslovnega procesa in njegovih posebnosti, nikakor ne morejo učinkovito opravljati svojega dela. To pa pomeni, da jih strateško vodstvo organizacij ne bo prepoznalo kot pomemben segment za uspešnost podjetij in bodo zelo hitro odrinjeni na kraj organizacijske strukture in s tem tudi na marginalizacijo dojemanja korporativne varnosti kot ene izmed pomembnih profesij v širšem družbenem okolju.

Mednarodne korporacije poslujejo v širšem mednarodnem okolju, ki jih že samo po sebi sili, da imajo funkcijo korporativne varnosti v večini primerov ustrezno urejeno. Seveda obstajajo tukaj določene organizacijske modalitete, ki so predvsem odvisne od poslovnega portfelja mednarodne korporacije in vplivov tveganj na nemotenost poslovanja. S tem pa je povezan tudi ugled in dojemanja potrebnosti korporativne varnosti. V nacionalnih okoljih, predvsem držav v tranziciji, ki so v okolje tržnega go-



*avtor je član Slovenskega združenja korporativne varnosti



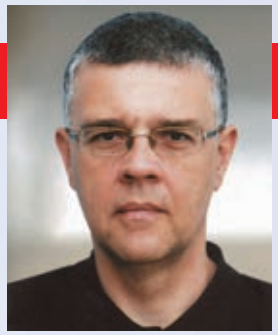
spodarstva vstopile po družbenih spremembah ob koncu 20. stoletja, pa je stanje korporativne varnosti še močno v fazi razvoja in iskanja ustreznega mesta v poslovnem okolju. Gre tudi za težave pri razumevanju vloge, poslanstva in nenazadnje odgovornosti strateškega managementa in posledično tudi korporativne varnosti kot osnovnega orodja za učinkovito obvladovanje tveganj v organizacijah, ki jih vodijo. Republika Slovenija je v tem okviru zaradi njene zaprtosti gospodarskega okolja pred vstopanjem mednarodnega kapitala dodatno hendikepirana pri razvoju korporativne varnosti, kot nujno potrebne profesije, ki je nujen predpogoj za zagotavljanje ustrezne prožnosti poslovnih organizacij za njihovo učinkovito poslovanje v zahtevnem mednarodnem globalnem okolju. Pomemben korak za dvigovanje pomena korporativne varnosti predstavlja nov magistrski program »Management korporativne varnosti«. Ta program bo zagotavljal pridobitev nujno potrebnih znanj, ki jih bodo korporativno-varnostni strokovnjaki potrebovali pri izvajanju svojih nalog v organizacijah in posledično s tem tudi dvigovanju svojega ugleda, ki se bo odražal v višji organizacijski umeščenosti te dejavnosti in seveda višjemu materialnemu statusu strokovnjakov s tega področja. Institut za korporativno varnostne študije in predvsem Slovensko združenje korporativne varnosti imata v tem okviru tudi izredno pomembno vlogo združevanja in tvorjenja sinergij na področju znanja in prenosa dobrih praks na področju korporativne varnosti.

Zavedati pa se moramo tudi, da tisto kar prihaja iz mednarodnega okolja ni nujno dobro ali slabo. Vedno je potrebno na določen proces pogledati s potrebne distance, ki nam bo omogočala realno oceno dobrih in slabih procesov. Seveda je zaželeno, da v naše okolje v čim večjem obsegu prevzemamo dobre prakse in izkušnje in se učimo na napakah, ki so jih naredili drugi. V mednarodnih korporacijah imamo nekaj odličnih strokovnjakov iz Slovenije, ki so pripravljeni prenašati ustrezna znanja v nacionalno okolje. To je potrebno sprejeti z odprtimi rokami. Izkoristiti pa bo potrebno tudi vsako priložnost, ki se bo ponudila na področju korporativne varnosti v mednarodnem okolju in pridobljena znanja preveriti v zahtevnih dinamičnih okoljih. Zavedati pa se je potrebno, da so v določenih državah v regiji že stopili nekaj korakov naprej, medtem ko smo se mi ukvarjali s fundamentalnimi nepotrebnimi zadevami. Kljub veliki kritičnosti javnega mnenja do prevzema Mercatorja s strani Agrokorja bomo zelo hitro videli ali lahko ta združitev pripomore k prenosu dobre prakse in sinergij delovanja na področju korporativne varnosti. Prvi signali kažejo na to dejstvo, da so določena velika podjetja v regiji daleč pred nami v miselnosti strateškega managementa o potrebnosti in vlogi korporativne varnosti.

Za konec je potrebno poudariti star slovenski rek »vsak je svoje sreče kovač«, kar v realnosti pomeni, da bo vpliv in vloga korporativne varnosti v celoti odvisna od vsakega posameznika, ki v svojem okolju predstavlja to profesijo. Znanje in veščine ter prodornost vsakega posameznika so tista pot, ki bo prinesla spoštovanje in ugled ter materialni status strokovnjakov korporativne varnosti. Nikoli ne pozabite osnovnih gesel Slovenskega združenja korporativne varnosti, ki govorijo »Skupaj smo močnejši in tako gradimo pot do uspeha« in »Ab uno disce omnes (po enem spoznanj vse)«. Samo vsi skupaj lahko pripomoremo, da bo pot razvoja usmerjena navzgor in za to je zaslužen in seveda odgovoren vsak posameznik.

Zaradi vsega navedenega vas pozivam, da v roke vzamete orodja, ki so vam na voljo in začnite skupaj z nami tlakovati svetlo prihodnost profesije, ki se ji reče »korporativna varnost«. Upamo, da bo naša pot vodila v pravi smeri brez odvečnih stranpoti. ■

Avtor: Dr. Dorijan Keržan / pomočnik direktorja Nacionalnega forenzičnega laboratorija



KAKO ZAGOTOVITI VARNOST LISTIN

Razvoj informacijske tehnologije je v zadnjih dveh desetletjih bistveno spremenil poslovno okolje in navade.

Dandanes je že težko najti resnega poslovneža, ki bi z nalivnim peresom pisal v z usnjenim ovitkom okrašen poslovni planer, saj je uporaba tabličnega računalnika neprimerno bolj preprosta in omogoča hkratno povezljivost s podatki, ki jih je treba kajpada vedno imeti pri roki. Temu se vse bolj prilagajajo tudi ponudniki informacijskih rešitev. A vendarle dragoceno nalivno pero in papir še nista v celoti izginila iz poslovnega okolja in verjetno je, da tudi še dolgo ne bosta. Težko si je namreč predstavljati podpisovanje pogodbe z aplikacijo na mobilnem telefonu ali s pametno kartico. Navsezadnje se tudi informacijski kriminal razvija tako hitro, da se na varnost informacijskih rešitev ni mogoče povsem zanesti. Kljub temu se zdi, da v poslovnem okolju hitro pozabljajo na prednosti nekaterih tradicionalnih oblik poslovnega dokumentiranja, zaradi česar pa se lahko kaj hitro podjetje znajde v položaju, ko zaradi neustreznega varovanja in hrambe svoje poslovne dokumentacije pride do poslovnih izgub.

V forenzični praksi preiskovanja dokumentov pogosto srečujemo prakso podjetij, da svojih listin ne hranijo več v fizični obliki, pač pa zgolj še v elektronski. Prehod na elektronsko hrambo dokumentov, zlasti podpisov, je lahko izveden na dva načina.

Prvi je uporaba podpisnih tablic za neposreden prenos podpisa v elektronsko obliko podpisa. V Republiki Sloveniji je na takšen način že urejeno podpisovanje dokumentov, ki so izdelani z laserskim graviranjem in je tako odpravljen sistem kartončkov, na katere so se nekoč lepile fotografije, prosilec pa jih je tudi lastnoročno podpisal. Z ukinitvijo kartončkov in njihove hrambe je tako celoten postopek izdaje dokumenta postal elektronski (tudi fotografijo prosilcu na Upravni enoti vrnejo). Podobno so podpisovanje denimo dvižnih lističev informatizirale nekatere banke, pa tudi trgovske verige za podpisovanje lastnih plačilnih kartic. Prednost takšnega poslovanja je prav gotovo v tem, da ni več skrbi s hranjenjem velikih kupov papirjev (ki so bili lahko tudi zelo majhni in tako precej neprimerni za hrambo, pri potrdilih iz POS terminalov pa se je dogajalo, da so s časom tako zbledeli, da so postali povsem neuporabni). Po drugi strani pa je v takšnih primerih težava, kadar pride do zlorabe. Podpis (ali rokopis) narejen na podpisno tablico je namreč s stališča preiskovanja pristnosti podpisov in rokopisov praktično neprimeren za identifikacijo. Za to je več razlogov. Najprej je treba opozoriti, da je podpis na tablico podpis na povsem drugačno površino kot jo ima papir. Papir ima teksturo in tako ustvarja drugačen upor pisalnemu sredstvu kot gladka površina tablice. K temu velja prišteti še to, da pisalo, s katerim pišemo na tablico, tudi samo zaradi tega, ker ni treba, da na podlagi pusti barvilo, tudi samo lahko spremeni upor, ki ga pri podpisovanju na papir skupaj povzročita papir sam kot tudi pisalno sredstvo. Druga pomembna razlika med podpisom na podpisni tablici in podpisom na papirju je v njegovi vizuelni predstavnosti. Ob pregledu podpisa na papirju namreč ne gre zgolj za oblikovno preiskavo, pač pa je omogočen tudi vpogled v dinamiko pisanja, (relativno) hitrost drsenja pisalnega sredstva po površini, pritisk na površino in podobno. Vse to so pomembni identifikacijski momenti pri morebitni preiskavi podpisa. Seveda je jasno, da načeloma vsaj nekatere, če ne večina, podpisnih tablic omogočajo morebiti še bistveno natančnejše meritve teh karakteristik (hitrost, pritisk ...), vendar teh značilnosti ne hranijo, tako da so za morebitno preiskavo izgubljeni, hkrati pa je treba vedeti, da bi morebitna dostopnost teh podatkov za preiskavo zahtevala enak način zbiranja primerjalnega gradiva, torej odvzem podpisov s pomočjo podpisne tablice. Iz navedenega pa izhaja še dodaten in morda največji problem podpisnih tablic. Pri zapisu na podpisno tablico ta podpis prenese v elektronsko obliko, pri čemer (spet pretežno) tablica shrani zgolj obliko podpisa, izgubijo pa se vsi dinamični vidiki pisnega akta (pritiski, smeri, hitrost ipd.). Nekatere tablice v procesu elektronskega arhivira-

Kljub temu se zdi, da v poslovnem okolju hitro pozabljajo na prednosti nekaterih tradicionalnih oblik poslovnega dokumentiranja, zaradi česar pa se lahko kaj hitro podjetje znajde v položaju, ko zaradi neustreznega varovanja in hrambe svoje poslovne dokumentacije pride do poslovnih izgub.



Nekatere tablice v procesu elektronskega arhiviranja podpise še dodatno »zgladijo«, tako da so s stališča forenzičnih preiskav tako povsem neuporabni.

nja podpise še dodatno »zgladijo«, tako da so s stališča forenzičnih preiskav tako povsem neuporabni.

Drugi način elektronskega hranjenja dokumentacije je optični zajem papirnih dokumentov z optičnim čitalcem ali kamero. Tovrstno hranjenje dokumentacije je v zadnjih letih razmeroma pogosto v poslovnem svetu, zlasti v poslovanju s strankami. V elektronsko obliko zajeti dokumenti imajo v primerjavi s podpisi na podpisnih tablicah drugačne značilnosti. Morda najpomembnejša je ta, da je listina v celoti zajeta ter tako ni na voljo zgolj podpis, pač pa tudi vsa periferija dokumenta, vključno z denimo štampiljčnimi odtisi. Kljub hitremu napredku aparatov, namenjenih za zajem, ki omogočajo vse bolj kvalitetne slike, je treba opozoriti, da tudi v tem primeru za preiskovalca listine (ne samo podpisa in rokopisa, pač pa tudi drugih lastnosti, kot so štampiljčni odtisi, prednatisnjeni listinski elementi, kot so logotipi ipd.) reprodukcija, bodisi na ekranu bodisi na papirju (če jo natisnemo) pri preiskavi močno omejuje, čeprav manj, kot v primeru podpisne tablice. Optični zajem je namreč pretežno dvodimenzionalen, preiskava podpisa in rokopisa pa pogosto temelji tudi na tridimenzionalnem modelu zapisa. Kljub temu je preiskava v takšnih primerih mogoča (enako velja tudi za fotokopirane dokumente), vendar se je treba zavedati, da je rezultat preiskave oz. mnenje o pristnosti ali nepristnosti podpisa (lahko pa tudi štampiljčnega odtisa) v takšnem primeru nujno relativiziran in podan z nižjo stopnjo verjetnosti. Za takšen pristop k tovrstno hranjenim dokumentom sta dva razloga. Eden je že navedeno dejstvo, da so značilnosti rokopisa oz. podpis na optično zajetem dokumentu slabše vidne, delno prikrite, delno pa zaradi značilnosti optičnega zajema nevidne, drugi razlog pa je v tem, da forenzični preiskovalec na optično zajetih (ali fotokopiranih) dokumentih preprosto ne more (vsaj večinoma) potrditi integritete same listine, saj ne more ugotoviti, ali ni morebiti dokument, ki ga preiskuje, sestavljen iz več dokumentov, podpis prenesen na listino od drugod (kar je pogosta obramba na sodišču) in podobno. Prav zaradi tega se mora forenzični strokovnjak v takšnih primerih vedno zaščititi z izjavo, da pač verjame v integriteto dokumenta oz. da o tem ne more podati nikakršnih ugotovitev. Vse to lahko bistveno oteži morebitne dokazovalne postopke v primerih, ko poslovne listine na tak ali drugačen način postanejo sporne. K temu je treba še dodati, da optično zajeti (ali fotokopirani) dokument ne omogoča preiskovalcu potrditi pristnosti štampiljčnega odtisa, prednatisnjenih logotipov in seveda varnostnih elementov papirja, kot je na primer vodni znak.

Morda je smiselno poudariti, da je elektronsko hranjenje listinskega gradiva pogosto zelo površno opravljeno, saj je hramba v črno-beli tehniki in izpis s tiskalnikom posledično zelo slabe kvalitete. Vsekakor se je v primeru odločitve za elektronsko hrambo koristno posvetovati tudi s strokovnjakom forenzične stroke, ki bo morda lahko svetoval, kako zajemati dokumente, če pa to ni mogoče, se velja držati nekaj enostavnih pravil. Listine, ki jih želimo hraniti elektronsko je treba vedno zajeti z barvno sliko, ki ohranja več značilnosti, kot črno-bela. Sliko je treba zajeti v razmerju ena proti ena, se pravi manjšanje slike ni dopustno. Slika naj bo zajeta z resolucijo najmanj 300 dpi, ki že omogoča določeno raven kakovosti, hrani pa naj se v formatu pdf ali jpg, ki zagotavljata razmeroma solidno kakovost zajete slike in ne zasedata preveč diskovnega prostora. V primeru, da dokument postane sporen, pa je koristno, da forenzični strokovnjak poleg tiskane verzije elektronsko hranjenega dokumenta na ustreznem nosilcu prejme tudi datoteko s sporno listino, kar bo omogočilo lažji pregled nekaterih značilnosti podpisa, rokopisa, štampiljčnega odtisa.

Pri odločanju za elektronsko hrambo listin je glavni argument običajno prihranek prostora, upoštevati pa je treba, da tudi elektronska hramba ne pomeni, da stroškov s hrambo ni, saj je strežniška in programska oprema, ki mora biti varnostno ustrezna, razmeroma draga. Morda ključna prednost takšne hrambe je njena enostavna uporaba ter hitra dostopnost, ki je arhiviranje papirja seveda ne more zagotoviti.

Racionalnost elektronske hrambe dokumentov je ena stran enačbe, na njeni drugi strani pa je tehtanje tveganj morebitnih kazenskih ali pravdnih postopkov, v katerih bi bilo treba dokazovati pristnost posameznega dokumenta, podpisa. Tehtanje teh tveganj in pripravljenost sprejemanja tveganj je seveda v domeni vsakega posameznega pravnega subjekta, nedvomno pa je, da pri dokumentih, ki lahko potencialno prinesejo velike izgube, velja ostati previden in konservativen glede hrambe. Prav gotovo je elektronska hramba smiselna tudi za te dokumente (vsaj s stališča racionalnosti in enostavnosti dostopanja do njih, a kadar gre za večja tveganja, je smiselno takšne dokumente hraniti tudi v originalni, torej papirnati verziji. Še več, kadar gre za dokumente z visokim tveganjem je smiselno, da so ti dokumenti morebiti narejeni na delno zaščitnem papirju (morda z vodnim znakom) oziroma vsaj na papirju s prednatisnjenim logotipom in ne z logotipom, narejenim s tiskalnikom. Če bodo morebitni ponarejevalci želeli ponarediti listino, ki ima logotip natisnjen z računalniškim tiskalnikom, jim bo ponarejanje bistveno bolj enostavno, kot če bi šlo za prednatisnjene vzorce, narejene s klasičnimi tiskarskimi stroji. Tudi sicer neredko prakso podjetij, da celo svoje žige (torej tisto, kar bi morali odtisniti s štampiljko) tiskajo s tiskalnikom, je treba opustiti. Dodatno pa velja podpisnikom listin svetovati, naj opustijo enostavne parafne podpise in se poskušajo podpisovati čim bolj individualizirano, saj je tudi enostaven podpis, ki sestoji iz kratke vijuge, povsem enostavno ponarediti. Skratka, nove informacijske tehnologije so v svet listin prinesle mnogo poenostavitev in racionalizacij, hkrati pa odprle vrata novim tveganjem oz. stara tveganja postavila na drugačne temelje. Pričujoči prispevek je želel opozoriti na nekatere probleme in tveganja, ki jih s seboj nosi elektronska hramba listin in kako se enostavno odzvati na njih, da se potencialna škoda zaradi morebitnega ponarejanja zmanjša in se storilca najde in pripelje pred sodišče. ■

Listine, ki jih želimo hraniti elektronsko je treba vedno zajeti z barvno sliko, ki ohranja več značilnosti, kot črno-bela.

Tehtanje teh tveganj in pripravljenost sprejemanja tveganj je seveda v domeni vsakega posameznega pravnega subjekta, nedvomno pa je, da pri dokumentih, ki lahko potencialno prinesejo velike izgube, velja ostati previden in konservativen glede hrambe.



Avtor: Dr. Brane Bertoncelj / Slovensko združenje korporativne varnosti



KAKO PREPOZNATI LAŽ — MIT ALI RESNIČNOST?

Tisoče let se že vodi borba med resnico in lažjo, med Dobrim in Zlim, saj sta dve polovici iste zadeve.

Laž je na načelni ravni moralno in etično nedopustna, posledično pa je tudi na določenih področjih družbene dejavnosti zakonsko sankcionirana. Kljub vsesplošni nezaželenosti se z njo žal vsakodnevno srečujemo. Zanimivo je, da ima od vseh nemoralnosti laž tudi svoj »praznik«, 1. april.

Proučevanje laži je podobno prodiranju v nevidni svet okoli nas, ki je v določenem smislu bolj zastrt in nepredvidljiv kot stvarnost, kot jo zaznavamo in vidimo. Ko je psihoanalitik Carl G. Jung dejal, da je **»Celovitost pri posamezniku odvisna od njegovega odnosa do svoje lastne sence«,** je s tem poudaril razumevanje temne strani posameznika. Pri tem je pomembno, da je vrednostno doživljanje samega sebe tudi ključ do vrednotenja vedenja drugih.

Posameznika, ki se ne bi nikoli zlagal, ni. Prav tako ni posameznika, ki bi vedno lagal. Lažemo vsi, razlikujemo se v pogostosti laganja in v tem, o čem, komu in kako dobro lažemo. Največja laž, ki jo lahko izgovorimo je, da nikoli ne lažemo. V vsakdanjem življenju se ta problem skrči predvsem na vprašanje, kako ugotoviti, kdaj nam nekdo laže.

Posameznika, ki se ne bi nikoli zlagal, ni. Prav tako ni posameznika, ki bi vedno lagal.

Laganje je namerna napačna predstavitev realnosti, skupna pa je vsem posameznikom in je zelo zapleten vedenjski pojav (Walters, 2003). Laž je pogosto opisana kot sebično dejanje, stvar osebne odločitve in je vedno zavestna.

Eden izmed vodilnih proučevalcev fenomena laži Ekman (1992) je definiral laž kot namerno odločitev, da bomo nekoga zavedli, ne da bi ga o tem prej obvestili. Nekateri avtorji (npr. Goleman, 1986; Thruman, 1999) pravijo, da lažemo tudi sami sebi. Laž ne predstavlja nujno popolnega izkrivljenja realnosti (Krauss, 1981). Laganje je opisano kot grožnja moralni družbi (Bok, 1978), negativen odnos v življenju (Stouthamer-Loeber, 1986), kot socialna spretnost (DePaulo in Jordan, 1982; Nyberg, 1993), kot pomemben osebni razvojni mejnik (Devilliers in Devilliers, 1978), obravnavano je na različnih področjih razvojne psihologije (Kashy, 1991; Reis in Wheeler, 1991; Tennen, Suls in Affieck, 1991) in socialne psihologije (npr. Fiedler, Semin in Koppetsch, 1991, Giles in Wiemann, 1993; Leets in Giles, 1997; Schnake in Ruscher, 1998; Semin in Fiedler, 1988; Ruscher, 2001). Avtorji so predlagali tudi razne vrste in oblike usposabljanja za prepoznavanje mikro izrazov izražanja čustev (npr. Ekman in Matsumoto, 2008; Matsumoto in Hwang, 2011), koristi usposabljanja za odkrivanje laži pa so raziskovali Landry in Brigham (1992); Porter et al. (2000) in Porter et al. (2010).

V bistvu lažemo zato, da bi se izognili kazni ali dosegli nagrado. Lažemo, da pred seboj in pred drugimi ne bi veljali za neuspešnega, nesposobnega, smešnega, neumnega, grdega ipd.

Med pomembnimi motivi laganja so: kazen in nagrada, potrebe po ohranjanju samopodobe, samospoštovanja, ugleda in spoštovanja drugih posameznikov (Hrnjica, 1990; Musek, 1993; Lamovec, 1994; Hayes, 1998). V bistvu lažemo zato, da bi se izognili kazni ali dosegli nagrado. Lažemo, da pred seboj in pred drugimi ne bi veljali za neuspešnega, nesposobnega, smešnega, neumnega, grdega ipd.

Različni avtorji (npr. Krauss, 1981) tudi govorijo o različnih vrstah laži kot so: bela laž (vljudnostna), namerno škodljiva in egoistična laž, aktivno laganje (izmišljanje informacij) in pasivno laganje (skrivanje informacij).

Obstajata dva osnovna načina laganja: prikrivanje in ponarejanje. Prikrivanje pomeni, da posameznik zadrži neke po-

datke, ne da bi dejansko rekel kaj, kar ne bi bilo res. Ponarejanje pa pomeni, da posameznik zadrži resnične podatke, napačne pa predstavi kot resnične.

Avtorji kot vzrok za laganje postavljajo strah, ki je najpogostejši motiv za laganje, v najslabši obliki pa želja, da bi nekoga osebno prizadeli. Vzrok je lahko tudi posnemanje odgovornih referenčnih posameznikov (v službi, doma, med prijatelji). Ko posameznik vidi lagati druge, še posebno, ko jim laž prinese določene koristi, postane bolj pripravljen lagati tudi sam.

Različni avtorji (npr. Krauss, 1981; Hollander, 1997; Vrij, 2000 v Gasar, 2004) se strinjajo, da obstajajo v laganju velike medosebne razlike. Laganje je naučeno, lažnivost pa relativno trajna značajska lastnost. Laganje je odvisno tako od osebnosti posameznika kot tudi od socialne situacije: motivov, odnosov z drugimi, konkretnih okoliščin, pritiskov ipd. (Umek, 1998).

Glede na vzrok laži so jo avtorji razdelili v tri skupine (DePaulo, v Vrij 2000): (1) laž o sebi: je tista, ki lažnivcu pomaga, da se pokaže v boljši luči ali da doseže določeno korist (približno polovica vseh laži), (2) laž o drugih: je tista, ki se uporablja z namenom, da bi druge prikazal v boljši luči, da jih ne bi prizadel (predstavljajo približno 25 odstotkov izrečenih laži in so izrečene posameznikom, ki so lažnivcu blizu) in (3) socialna laž: je tista, ki koristi širši družbi. Posameznik laže tudi za dobre medsebojne odnose (te laži zavzemajo 25 odstotkov).

Ekman (1985) opredeljuje čustva, ki jih najpogosteje čuti posameznik, ki laže. To so strah, krivda in vznemirjanje. Najpogostejši je strah pred odkritjem, medtem ko občutek krivde po jakosti lahko varira. Vznemirjenje se kaže z znaki veselja, ko smo uspešno prikazali laž kot resnico.

Tisti, ki laže, se zaveda, da lahko sogovornik opazuje njegovo govorico telesa, da bi presodil, ali govori resnico ali ne, zato poskuša kontrolirati svoje vedenje (Vrij, 2008, po Buller in Burgoon, 1996; Krauss, 1981). To pa ni enostavno. Nekatere znake je skoraj nemogoče nadzirati, ker so vezani na doživljanje močnih čustev ali visokega stresa (Vrij, 2008, po Ekman, 1985/2001).

Posameznik razpolaga z najhitrejšim sistemom za dojemanje sveta okoli sebe, imenuje se amigdala in se nahaja v možganih. Njena glavna naloga je ocenjevanje drugih posameznikov. V nas ustvarja občutke o sočloveku, s katerim stopamo v stik. Strah pred sočlovekom se na primer sproži v povprečno v dveh stotinkah sekunde.

Posameznikova inteligenca je ključnega pomena za odkrivanje laži, zato je bistvenega pomena, da zaznavamo, kdaj je pridobljeni podatek napačen. Rezultati raziskav so pokazali, da ko posameznik laže, se pojavijo prek več telesnih kanalov različni vedenjskim izrazi. Štiri od teh kanalov so nebesedni (mimika, geste in govorica telesa, glas in glasovni slog). Peti kanal pa je besedna izjava. Raziskave v zadnjih 30 letih kažejo, da je povprečen posameznik statistično nekoliko boljši od naključja pri ugotavljanju laži, ne pa tudi praktično boljši. Pregled nad sto raziskav kaže, da je natančnost ugotavljanja laži približno 57 odstotkov Kraut (1980, v Vrij, 2000).

Kako dobro lahko prepoznamo laž? Večina posameznikov je neizkušena v zaznavanju laži (Vrij, 2000). Raziskave (DePaulo, 1996) pa so pokazale, da zaznamo samo nekatere laži drugih. Govorica telesa predstavlja večino medosebne komunikacije in je smiselno uporabna tudi za prepoznavanje laži. Mehrabian (1971) je z raziskavami ugo-





tovil popularno oznako 7—38—55. Celotno sporočilo sprejemamo z besedami (7%), preko glasu (38%) in 55% pa preko govorice telesa. Povprečnega lažnivca najbolj pogosto izda povišano čustveno vzburjenje (Krauss, 1981; Lieberman, 1998; Vrij, 2000). Lažnivec tudi pogosto kaže znake distresa (Umek, 1998). Ker so fiziološke spremembe ob čustvenem vzburjenju povezane z delovanjem avtonomnega živčnega sistema, ki deluje neodvisno od zavestne volje posameznika, jih večina ne zna dobro nadzorovati. Veliko posameznikov je prepričanih, da lahko poštenost sogovornika ugotovijo s pogledom v njegove oči. Nekatere raziskave so sicer pokazale, da to splošno pravilo v nekaterih primerih drži, vendar pa še zdaleč ni zadosten indikator za kvalitetno ugotavljanje laži.

Izdelane so bile številne raziskave o obnašanju posameznika, ki laže, vendar niso odkrili samo enega besednega, nebesednega ali psihološkega znaka, ki bi bil zadosten dokaz, da nekdo laže (npr. Vrij, 2000; MacLaren, 2001; Kleiner, 2002; Vrij, 2004, po Ben-Shakhar in Elaad, 2003; DePaulo, Lindsay, Malone, Muhlenbruck, Charlton in Cooper, 2003). Z drugimi besedami, ne obstaja ničesar takšnega kot je efekt »Ostržkovega nosu«. Pri sprejemanju prehitrih sklepov o laganju pa moramo biti previdni, saj je to zadnja možnost, ko smo vse druge izključili.

Ko proučujemo raziskave, ki so bile izvedene na področju prepoznavanja laži in laganja, lahko (1) dobimo vtis, da ni nič čudnega, da se veliko medosebnih odnosov na različnih področjih družbenega življenja neustrezno konča, če pa je več kot 60 odstotkov vsega, kar si izrečejo odrasli med seboj, večja ali manjša laž; (2) na srečo (in zadovoljstvo) pa imamo večino dela in življenja komunikacijo s poštenimi posamezniki.

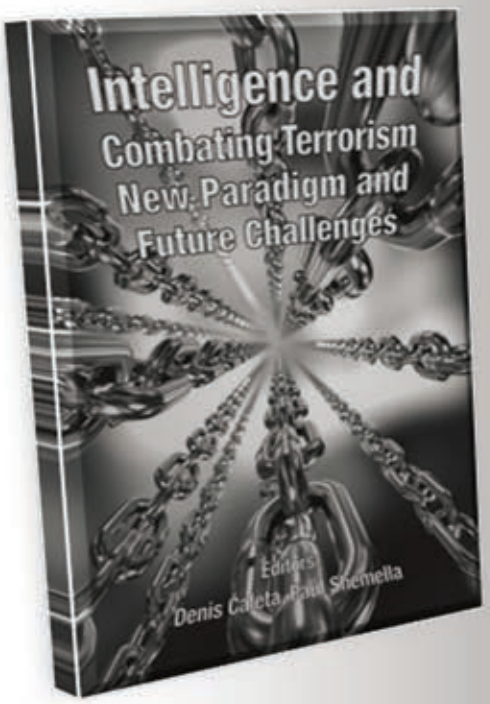
Na vprašanje: »Kako prepoznati laž — mit ali resničnost?« je avtorjem skupno prepričanje, da je to mogoče prepoznati. Razmerje med poštenostjo in nepoštenostjo temelji na dveh vrstah spodbud: (1) imamo radi koristi od laganja (razumska ekonomska motivacija); (2) sebe želimo videti brez slabosti (psihološka motivacija); vprašanje je, kako ta dva vidika uskladiti? Nekateri pravijo, da s tem, ko si dovolimo drobne laži, nismo daleč od velikih — takih, ki lahko povsem uničijo poslovno zaupanje, partnerstvo, prijateljstvo, zaupanje v starše, zaupanje v javne avtoritete ipd. Izguba zaupanja je boleča, Friederich Nietzsche je zapisal: »Nisem jezen, da si mi lagal, jezen sem, da ti od zdaj naprej ne morem verjeti.«

Laž bo žal še nadalje prisotna v delu in življenju ter se ji ne moremo izogniti. Vprašanje je tudi, ali smo pripravljeni na življenje polno resnice in iskrenosti, v svetu brez laži? Za preprečevanje laganja moramo predvsem storiti korak k sebi, v notranji stik z etiko in moralo, saj laganje izraža veliko stisko posameznika.

Več o tej temi bo predstavljeno na naslednji mednarodni konferenci o korporativni varnosti. ■

ICS PUBLIKACIJE - NOVOST





www.ics-institut.si

info@ics-institut.si

ICS

Institute for Corporative Security Studies



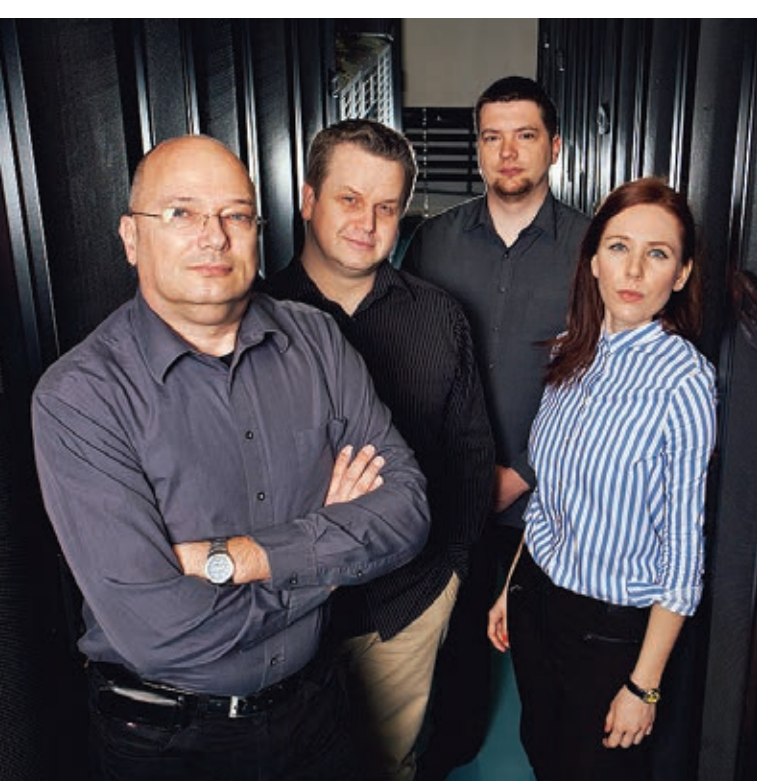
Avtor: Jasmina Mešič*/ Nacionalni center za posredovanje pri omrežnih incidentih SI-CERT**



VARNOST NA INTERNETU - NAJŠIBKEJŠI ČLEN JE UPORABNIK

V zadnjih letih opažamo velik porast spletnih prevar, ki ciljajo na podjetja. Goljufi v skrbno sestavljenih sporočilih obljubljalo neverjetne poslovne priložnosti, ki lahko podjetnikom pomagajo v težkih časih.

Izzivi, s katerimi se danes soočajo strokovnjaki za informacijsko varnost, še nikoli niso bili tako raznoliki. Na eni strani razvoj sofisticiranega programskega orožja, ki lahko onesposobi jedrsko elektrarno, na drugi strani pa za dosego cilja niso potrebni super napredni virusi, saj zadostujejo že preproste tehnike socialnega inženiringa. Slovenija ni izjema, saj se na nacionalnem centru za posredovanje pri omrežnih incidentih SI-CERT soočamo tako z naprednimi ciljanimi grožnjami kot tudi različnimi oblikami spletnih prevar. Od leta 2009 beležimo strmo rast različnih oblik spletnih goljufij, socialnega inženiringa in kraje identitete. Danes nam goljufi ne ponujajo več nigerijskih shem le prek elektronskih sporočil, ampak iščejo žrtve tudi prek forumov, družbenih omrežij ali SMS-sporočil. Razmah spletnega nakupovanja pomeni tudi razmah lažnih spletnih trgovin in prevar prek spletnih oglasnikov. Rdeča nit omenjenih primerov je dejstvo, da lahko spletni goljufi nepozornega, preveč zaupljivega uporabnika tudi finančno oškodujejo.



Slika 1: Nacionalni odzivni center SI-CERT

Zato smo na SI-CERT leta 2011 zasnovali nacionalni program **Varni na internetu, ravno z namenom ozaveščanja širše javnosti glede varne uporabe interneta** in prepoznavanja tveganj. Naše delo temelji na preventivnemu delovanju in izobraževanju spletnih uporabnikov, saj tehnična zaščita predstavlja le minimum omrežne higiene. Izkaže se, da pri mnogih spletnih prevarah, še tako napreden antivirusni program ne bi preprečil škode in zagotovil varnosti, saj je (pre)pogosto v verigi informacijske varnosti **najšibkejši člen ravno končni uporabnik**. **Najboljši recept je kontinuirano izobraževanje spletnih uporabnikov in ne slepa zaverovanost v programske rešitve**. Vsebine našega portala Varni na internetu naslavljajo široko slovensko javnost, ciljamo predvsem na odrasle spletne uporabnike, ki že uporabljajo storitve elektronskega bančništva in spletnih trgovin. Poseben sklop vsebin pa namenjamo podjetnikom, saj predvsem manjša podjetja, obrtniki, društva zaradi omejenih kadrovskih ali finančnih resursov pogosto kar sami skrbijo za svoj »IT-oddelek.

*Koordinatorka programa ozaveščanja Varni na internetu, ki ga izvajajo na nacionalnem centru SI-CERT
**Korporativni član Slovenskega združenja korporativne varnosti

Podjetniki vse pogosteje tarče spletnih goljufov

Na SI-CERT kot največjo grožnjo manjšim podjetjem še vedno izpostavljamo zelo slabo vzdrževane spletne strani, ki predstavljajo lahke tarče za hekerje. V zadnjih letih pa opažamo velik porast spletnih prevar, ki ciljajo na podjetja. Goljufi v skrbno sestavljenih sporočilih obljubljalo neverjetne poslovne priložnosti, ki lahko podjetnikom pomagajo **v težkih časih.** Naštevamo le nekaj primerov, ki smo jih obravnavali, univerzalnega nasveta, kako ločiti goljufivo od legitimne ponudbe, žal ni. **Vsekakor pa so sumljive velike obljube o neverjetnih zaslužkih, ki so le nekaj klikov stran.**

Odlična poslovna priložnost

Slovensko podjetje je kontaktiral Mohammed Kebbay iz katarskega Ministrstva za subvencije in islam. Ponudil jim je sodelovanje na javnem razpisu za nakup 50.000 kosov njihovega



THE ISLAMIC STATE OF QATAR
MINISTRY OF ENDOWMENTS AND ISLAMIC AFFAIRS
PROJECT PROCUREMENT DIVISION
Al Funduq St., Doha, Qatar P. O. Box 422
Website: http://www.islam.gov.qa
Phone/Fax: +97444470777, 974 4470700

Our Ref:.....RPP/CTC/005..... Doha:. 05/05/2014

IONEX D. O. O
Slomskova 25 SI-1000
Ljubljana Slovenija, EU

Attn:The President,

PROFORMA INVOICE APPROVAL

By the power vested upon me as the Honourable Chairman of the Public Procurement Division of the Ministry of Endowments and Islamic Affairs, Islamic State of Qatar, I hereby unequivocally approved the items as expressed in Proforma Invoice Number: 10337/14 dated April, 15th 2014 to the Department of Public Procurement.

We have adequately carried out a thorough study on your products and came to a conclusion that it is indeed in conformity with the required Ministerial need.

The items are as specified in your Proforma Invoice Number: 10337/14 dated April, 15th 2014 respectively.

The total value of the said Proforma Invoices is €1,843,000.00 (One Million Eight Hundred and Forty Three Thousand Euro) only.

Subsequent upon this Proforma Invoices Approval, the Legal Department of this Board is processing the Contract Agreement, which shall be signed by both parties before the execution of the payment into your bank account.

The Contract Amount will be transferred to your nominated bank account when all requisite procedures are completed. The Honourable Chairman of Public Procurement Department hereby approved your Invoice.

C O N G R A T U L A T I O N S !!!

Yours faithfully,

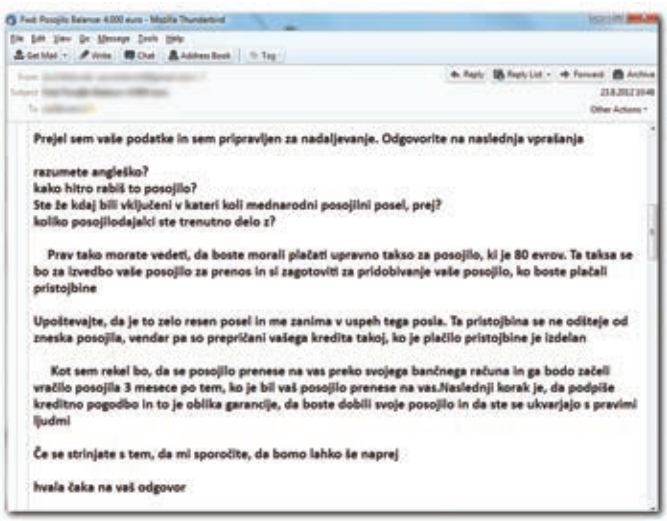
Dr. Muhammed IBN Hussein
Executive Chairman
Central Tender Committee

Slika 2: Lažno potrdilo o naročilu

izdelka, vrednost razpisa je bila 2 milijona evrov. Po zelo hitrem postopku je bilo podjetje tudi izbrano na razpisu, v podpis pa so jim poslali množico obrazcev in pogodb. Na srečo so se iz podjetja po nasvet obrnili na nas, kjer smo v sodelovanju s kolegi iz Katarja hitro ugotovili, da gre za goljufijo. Z malce raziskovanja smo prišli do podatka, da prevara izvira iz Gane. Kakšno škodo bi podjetje utrpelo, ko bi poslalo tistih 50.000 kosov, raje ne razmišljamo. V tem primeru se je poskus goljufije srečno končal, žal pa ni vedno tako. Na nas se je po pomoč obrnilo tudi podjetje, ki je pri kitajskem prodajalcu, s katerim so že uspešno sodelovali, naročilo in plačalo celoten ladijski zabojnik polizdelkov. Kasneje se je izkazalo, da je v njihovo komunikacijo s kitajskim podjetjem vdrl neznanec, našemu podjetju poslal podatke o novem bančnem računu, kjer pa se je sled denarja povsem izgubila.

Krediti prek spleta

Na različnih slovenskih spletnih straneh, forumih in oglasnikih so pogoste mamljive ponudbe ugodnih kreditov. Eden takšnih se glasi: *"Ali ste v finančni krizi? Ali ste že zavrnili banke za posojilo? Ali potrebujete denar nujno? Ali potrebujete posojilo za širitev vašega podjetja? Ste iskali posojilo? Ste prišli na pravo mesto. To posojilo je 100% zagotovljena. Contact me zdaj in dobili kakovostne storitve. Gospa Ebis Vivian (finaid45@hotmail.com)"*



Prejel sem vaše podatke in sem pripravljen za nadaljevanje. Odgovorite na naslednja vprašanja

razumete angleško?
kako hitro rabiš to posojilo?
Ste že kdaj bili vključeni v kateri koli mednarodni posojilni posel, prej?
koliko posojilodajalci ste trenutno delo z?

Prav tako morate vedeti, da boste morali plačati upravno takso za posojilo, ki je 80 evrov. Ta taksa se bo za izvedbo vaše posojilo za prenos in si zagotoviti za pridobivanje vaše posojilo, ko boste plačali pristojbine

Upoštevajte, da je to zelo resen posel in me zanima v uspeh tega posla. Ta pristojbina se ne odšteje od zneska posojila, vendar pa so prepričani vašega kredita takoj, ko je plačilo pristojbine je izdelan

Kot sem rekel bo, da se posojilo prenese na vas preko svojega bančnega računa in ga bodo začeli vračilo posojila 3 mesece po tem, ko je bil vaš posojilo prenese na vas.Naslednji korak je, da podpiše kreditno pogodbo in to je oblika garancije, da boste dobili svoje posojilo in da ste se ukvarjajo s pravimi ljudmi

Če se strinjate s tem, da mi sporočite, da bomo lahko še naprej

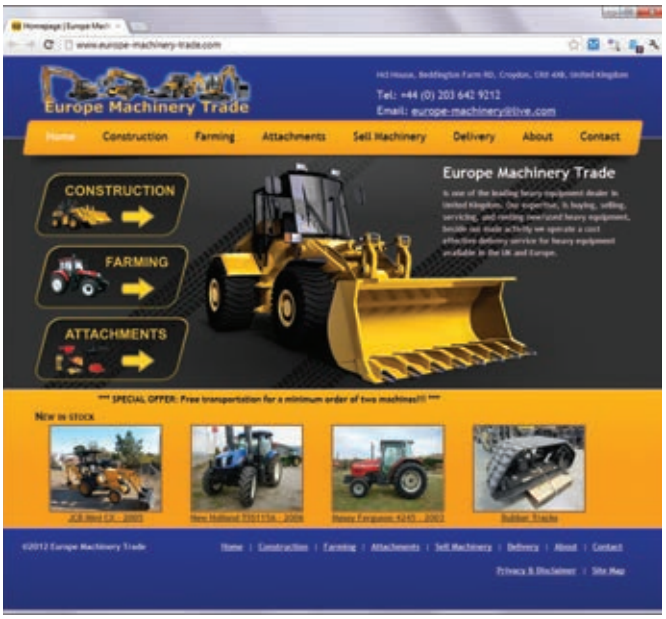
hvala čaka na vaš odgovor

Slika 3: Primer komunikacije spletnega goljufa

Prek objavljenega e-mail naslova smo kontaktirali ga. Vivian in še isti dan dobili odgovor, da lahko dobimo ugoden kredit. V naslednjem koraku smo morali posredovati svoje osebne podatke, telefonsko številko in višino mesečnega dohodka. Torej vse tisto, kar bi tudi sicer pričakovali pri najemu kredita. Posredovali smo izmišljene podatke in telefonsko številko. V naslednjem koraku so zahtevali plačilo stroškov odobritve kredita, in sicer naj bi »pristojbino« v višini 100 evrov plačali **prek sistema Western Union. Gre za plačilni mehanizem, ki ne omogoča sledenja transakciji in je ravno zato priljubljeno orodje spletnih goljufov.** Nato smo prekinili vso komunikacijo, saj je naš eksperiment uspel, dokazali smo vse znake klasične nigerijske prevare.

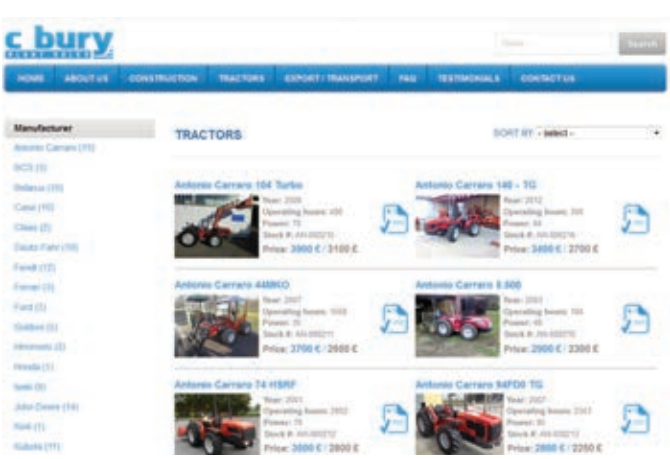
Super ugodni spletni nakupi

Stari bager je sedaj dokončno »crknil« in nujno potrebujete novega, sicer bo delo zastalo. Ustrezno mehanizacijo dandanes lahko najdete tudi na internetu in to po cenah, kjer tudi z vključenim prevozom celo prihranite. Na prvi pogled nas na spletu do super kupčije loči le nekaj klikov, vendar se lahko hitro zgodi, da za ponudbo pravzaprav stoji spletni goljuf. V lovu za dobro ceno lahko hitro naletimo na **lažno spletno trgovino, ki pa je le kulisa z lepimi fotografijami, za spletno predstavitvijo pa ne stoji legitimno pod-**



Slika 4: primer lažne spletne trgovine, ki je prodajala bagre

jetje. Tudi na SI-CERT smo bili presenečeni nad številom prijav ogoljufanih kupcev, ki so prek lažne trgovine »Europe Machinery Trade« kupovali bagre. Kljub našemu obvestilu ponudniku gostovanja in posledičnemu umiku strani se je ista lažna trgovina še nekajkrat uspešno pojavila v malce spremenjeni obliki in s spremenjenim imenom. V preteklem letu smo tako obravnavali veliko prijav ogoljufanih kupcev bagrov in drugih delovnih strojev, ki so že vplačali več 10.000 €, in še mnogo več prošenj za nasvet potencialnih kupcev, ki so se ustavili tik pred nakazilom denarja. V zadnjem času pa smo ponovno naleteli na več lažnih trgovin, ki prodajajo delovne stroje, tudi preko oglasov na slovenskih portalih. Zato previdno, naučite se brati super ponudbe tudi med vrsticami.



Slika 5: Neverjetno nizke cene so znak za previdnost, primer lažne spletne trgovine s traktorji

Tuje podjetje želi registrirati vašo domeno

Kitajsko podjetje, ki se ukvarja s prodajo domen, vas obvešča, da so dobili zahtevek za registracijo domene vašega podjetja. Ker so prijazni, vam omogočajo, da imate kot lastnik podjetja ali blagovne znamke, prednost pri registraciji. V takšnem primeru ne moremo 100 % zatrditi, da gre za prevaro, prav gotovo pa gre, za zelo milo rečeno, **nepošteno poslovno prakso**, saj vas **želijo prisiliti, da registrirate domeno pri nekem drugem registrarju.** Vendar pa vam kitajski ali katerikoli drug registar v naslednjem koraku ponudi registracijo pod tujimi vrhnjimi domenami, recimo .cn (Kitajska) ali .co (Kolumbija), ne pa pod tistimi, za nas najbolj aktualnimi, npr. slovensko .si ali .com domeno. Č**e imate domeno vašega podjetja** že registrirano pod .si ali .com, je drugo podjetje pod isto vrhnjo domeno ne more registrirati, torej ste lahko brez skrbi.

V isto skupino prevar, bolje rečeno zavajanj, uvrščamo **tudi sporne vpise v registre podjetij.** Po elektronski ali tudi navadni pošti prejmete dopis, ki vam ponuja vpis podjetja v register podjetij, ki na prvi pogled izgleda kot nek uraden register. Pogosto uporabljajo znak Evropske unije, v resnici pa gre za povsem zaseben in neznan register podjetij. **V drobnem tisku pa se skriva podatek, da morate vpis plačati.** S podpisom pogodbe se lahko tudi zavežete, da boste za vpis plačevali naslednjih 10 let! ■

Ključna vodila spletne varnosti za podjetnike:

1. Preverite, ali naslov sogovornika v elektronskem sporočilu ustreza osebi oziroma instituciji, ki jo predstavlja. Če v komunikaciji banka, podjetje, spletna trgovina ali evropska institucija, uporablja brezplačen e-naslov, npr. gmail, hotmail, blumail, je to znak za previdnost.
2. Nikoli ne plačujte z Western Union! Gre za plačilni mehanizem, ki ne omogoča sledenja transakciji in je zato priljubljeno orodje spletnih goljufov.
3. Brskajte za informacijami. Če prejmete super poslovno ponudbo, ki izrazito odstopa od ostalih, poskušajte pridobiti **čimveč informacij** o prodajalcu oz. podjetju, ki vas je kontaktiralo. Naj bo Google vaš najboljši prijatelj, informacije iščite tudi na forumih, kjer se zelo hitro širijo opozorila s strani opeharjenih strank ali kupcev.
4. Presodite, ali razlika v ceni nakupa pri ponudniku v tujini odtehta tveganje, ki ga pri tem prevzamete. Predvsem pa zelo previdno pri nakupih izven EU, saj slovenska oz. evropska zakonodaja ne seže do Kitajske ali Indije.
5. Goljufije in oškodovanja prijavite policiji. Na banki poskusite preklicati morebitna nakazila. Za tehnično pomoč pri izsleditvi pošiljatelja elektronske pošte ter lokacije spletnega mesta se obrnite na info@varninainternetu.si. ■

Avtor: mag. Matjaž Drev / državni nadzornik za varstvo osebnih podatkov pri Informacijskem pooblaščencu*



»BYOD« IZ PERSPEKTIVE NADZORA IN ZASEBNOSTI

V zadnjih letih se je na področju informacijsko komunikacijske tehnologije (IKT) ob konceptih računalništva v oblaku in interneta stvari, vse pogosteje začel uveljavljati izraz BYOD. Gre za kratico, ki v angleškem jeziku pomeni »(B)ring (Y)our (O)wn (D)evice«, ali po naše, »prinesi svojo napravo.«

Osnovna ideja je preprosta, zaplete se pri izvedbi v praksi. Gre za težnjo, da bi zaposleni namesto službenih računalnikov, tablic in pametnih telefonov, uporabljali svoje zasebne naprave. Tak pristop sicer ni v celoti izviren, tako kot tudi ni bilo v celoti izvirno računalništvo v oblaku. Je pa vsekakor nova izrazita težnja po »hibridizaciji« službenih omrežjih z zasebnimi IKT napravami. Če smo do zdaj večinoma še ločevali službena in zasebna informacijska sredstva, se zdi, da takšno razmejevanje nenadoma ni več v modi.

Kar seveda ni nujno slabo, še posebej, če prisluhnemo (in verjamemo) tržnikom, ki vneto zagovarjajo prednosti BYOD v praksi. Vendar se je ob tem potrebno zavedati neizbežnih slabosti, zlasti z vidika zasebnosti uporabnikov informacijskih naprav. Pri »klasičnem« modelu deljenja na službeno in zasebno, ki se je odražal tudi tako, da je zaposleni na delovnem mestu uporabljal službeni računalnik, je skozi leta pravne prakse postalo bolj ali manj jasno, do kje delodajalec lahko izvaja zakonit nadzor, kje pa je ta meja presežena in že lahko gre za kršitev zakonodaje s področja varovanja osebnih podatkov. S širjenjem brezplačnega dostopa do interneta prek brezžičnih dostopnih točk, cenitvijo prenosnih računalnikov, tablic in »pametnih« telefonov, se je možnost vpetosti v službeno omrežje »kjerkoli in kadarkoli« močno povečala. Po eni strani so delodajalci spodbujali idejo dela iz oddaljene lokacije, ker je tako mogoče povečati storilnost in dosegljivost zaposlenih, po drugi strani pa so tudi zaposleni zagovarjali tak pristop, saj so se lahko, če so želeli opraviti svoje delovne naloge, pogosto izognili vožnji v službo in ždenju v (pogosto prenatrpanih) pisarnah. Razen tega se je številnim delodajalcem domislica, da jim ne bo potrebno kupovati službenih računalnikov in telefonov, ker bodo zaposleni pač uporabljali svoje lastne naprave, zdela mamljiva še z ekonomskega vidika. Kakorkoli že, zasebni sektor se je začel navduševati nad idejo hibridizacije službenih in zasebnih IKT sredstev, javni sektor pa se zaradi svojega konservativnega predznaka zaenkrat še izogiba tej noviteti. Dejstvo ostaja, da se o BYOD vse več govori, prav tako se osnovno idejo vse pogosteje uporablja v praksi. Premislek o prednostih in slabostih je zato nujen.

Vendar velja poudariti, da je tak premislek izrazito problematičen zaradi vsaj dveh razlogov. Po eni strani je ideja BYOD še premlada, da bi jo lahko pretresali s perspektive večletnih izkušenj, po drugi strani gre tudi za modno muho (pomislimo samo kako se je in se še povzdiguje ra-



*Korporativni član Slovenskega združenja korporativne varnosti

čunalništvo v oblaku), ki obljublja veliko, vendar pa mora realnost šele pokazati ali se bodo obljube tudi zares uresničile, in če da, do kakšne mere.

Kot je bilo že omenjeno, zagovorniki ideje BYOD med glavnimi prednostmi novega organizacijsko tehničnega pristopa poudarjajo nižje stroške za delodajalca, večjo produktivnost zaposlenih, večjo mobilnost zaposlenih, in nenazadnje tudi večje zadovoljstvo zaposlenih. Naštete prednosti se na prvi pogled zdijo mamljive, toda ob natančnejšem premisleku se pokažejo tudi slabosti, ki jih ne gre spregledati. Stroški so za delodajalca, ker mu pač ni potrebno kupiti računalnikov ali telefonov, resda nekoliko nižji, toda hkrati se lahko povečajo stroški vzdrževanja in varovanja tako raznovrstnega informacijskega sistema. Prav tako je vprašljivo povečanje produktivnosti zaposlenih, če delajo od doma. Ni dvoma, da bodo nekateri bolj produktivni, hkrati pa bodo tisti, ki so po naravi bolj lenobni in za resno delo potrebujejo nadzor in palico, morda manj produktivni.

Iskanje objektivnih odgovorov na zapisane dileme bo terjalo več resnih empiričnih raziskav. Zaenkrat smo pri iskanju odgovorov v veliki meri omejeni na ugibanje in intuicijo.

Je pa res, da je mogoče podoben očitek, torej premalo empirije in preveč špekulacije, uporabiti tudi tedaj, ko pretresamo slabosti v zvezi z idejo BYOD. Kljub pomisleku je potrebno izpostaviti slabosti, ki izvirajo iz uporabe zasebnih informacijskih naprav v službenih omrežjih, čeprav drži, da bo šele praksa pokazala ali so nevarne posledice omembe vredne oziroma celo prevladajo nad prednostmi, ali pa gre zgolj za preveč zaskrbljeno razmišljanje. Slabosti je že na prvi pogled mogoče zaslutiti na področju varnosti in nadzora nad informacijami. Je varovanje razvejanega informacijskega »ekosistema«, ki ga v primeru BYOD sestavlja precej bolj raznolik nabor zasebnih računalnikov, dlančnikov in telefonov, primerljivo z varovanjem »klasičnega« homogenega informacijskega omrežja? Je mogoče zagotavljati ustrezno raven informacijske varnosti v »hibridnem« omrežju, ki ga sestavljajo IKT elementi v zasebni in delodajalčevi lasti? Kako zagotoviti, da bo uporabnik na svoji lastni napravi redno posodabljal zaščito pred škodljivo programsko kodo? Kako zagotoviti, da bo požarni zid na takšni napravi ustrezno nastavljen? Vse to se na prvi pogled zdi preprosto tehnično opravilo, toda kaj storiti, če zaposleni ne bo sistemskim administratorjem dovolil (sicer dobronamernega) posega na svoji zasebni IKT napravi? Kdo bo v teh primerih nudil uporabniško podporo? Bo to delodajalec? Bo zaposleni prepuščen lastni (ne)iznajdljivosti?

Ob tem kratkem nizu varnostnih dilem se neizbežno zastavlja še vprašanje zasebnosti in nadzora. Dejstvo je, da imamo v delovnih razmerjih soočenje vsaj dveh interesov. Na eni strani je prisoten interes delodajalca, ki želi določeno (čim večjo) stopnjo nadzora nad lastnimi IKT napravami in nad informacijami, ki se pretakajo prek službenega omrežja. Na drugi strani pa obstaja interes zaposlenega po določeni stopnji zasebnosti. Med posameznimi kulturami so priča-



kovanja glede enega in drugega različna, kar je bolj konkretno opazno v nacionalnih in nadnacionalnih zakonodajah, ki urejajo varovanje osebnih podatkov in širšo pravico do zasebnosti. V ZDA denimo je zaposleni bolj ali manj v celoti prepuščen nadzoru delodajalca, v EU je slika drugačna, zaposleni ima namreč pravico do pričakovane zasebnosti tudi na delovnem mestu.

Razmejitev med nadzorom in zasebnostjo še zdaleč ni enostavna, tudi zato ne, ker lahko delodajalčev poseg v zasebnost zaposlenih v določenih primerih že predstavlja kršitev zakonodaje o varstvu osebnih podatkov. Ugotovljeni prekrški se lahko kaznujejo tudi z globami, ki so v nekaterih primerih precej visoke, zato je v osnovnem interesu delodajalca, da ve kje je meja, ko je nadzor nad zaposlenimi še dopusten. Pri klasičnem modelu službenih IKT sredstev je bila ta razmejitev jasna, nenazadnje smo ločnico v Sloveniji iskali tudi na podlagi dolgoletne inšpekcijske prakse Informacijskega pooblaščenca. Zato pa se meja, ko gre za mešano uporabo službenih in zasebnih IKT sredstev, kar je bistvo BYOD, zelo zabriše. V tem trenutku obstaja več (neodgovorjenih) vprašanj kakor odgovorov. Nekaj takšnih vprašanj zgolj za okus: Bodo uporabniki na svojih zasebnih napravah uporabljali dva uporabniška profila, enega za službene, drugega za zasebne zadeve, ali pa bo vse skupaj zmešano na enem profilu? Bo delodajalec imel pravico do dostopa do službeno pomembnega dokumenta, če bo zaposleni, ki bo hkrati lastnik naprave, tak poseg odklonil? Kaj se bo zgodilo s službenimi podatki na zasebni napravi zaposlenega ob prenehanju delovnega razmerja? Kje se bo začrtala meja, ko bo tehnični poseg sistemskih administratorjev še mogoče tolmačiti kot nudenje pomoči uporabnikom in ne nadzor nad delom zaposlenih? Odgovore bo potrebno (iz)najti. Pravna praksa in teorija bo to slej ali prej storila, toda zaenkrat je koncept BYOD v Sloveniji še preveč svež, da bi bilo mogoče podajati jasne in nedvoumne odgovore, ki niso veljavni zgolj danes, pač pa bodo veljavni tudi čez eno leto. Tisti pogumni in napredni delodajalci, ki ta trenutek drzno uvajajo koncept BYOD v svojo vsakdanjo prakso tvegajo, da zabredejo v pravno sivino. Meja, ko gre lahko že za kršitev zakonodaje o varovanju osebnih podatkov, je zato nevarno blizu.

Kljub vsem naštetim pomislekom in dilemam, se ideja BYOD preveč bohoti in krepi, da bi jo bilo mogoče z malomarnim zamahom roke odriniti na rob. Ker

V ZDA denimo je zaposleni bolj ali manj v celoti prepuščen nadzoru delodajalca, v EU je slika drugačna, zaposleni ima namreč pravico do pričakovane zasebnosti tudi na delovnem mestu.

ne gre za slovensko posebnost, pač pa za izraz svetovnega trenda, bodo spremembe neizbežne, zato je bolj kakor o tem ali je uporaba izhodišč, ki izvirajo iz BYOD koristna ali ne, smotrno razmišljati o ustrezni prilagoditvi. Ta ne pomeni nekritičnega sprejemanja prednosti ali zaskrbljenega tuhtanja o slabostih. Prav nasprotno, iskati je potrebno pragmatično ravnotežje, ki bo drugačno »od primera do primera«. Tam kjer potrebe po visoki stopnji varovanja informacij ni, zaposleni pa si lahko privoščijo večjo stopnjo zasebnosti oziroma je interes delodajalca po nadzoru majhen, uporaba zasebnih naprav ni problematična. Kjer pa iz narave dela izhaja zahteva po strožji varnosti in nadzoru, se zdi bolj preudarno o(b)stati pri »klasičnem« modelu in počakati, da se v zvezi s prakso uporabe BYOD izkristalizirajo jasni odgovori na zgoraj našteta vprašanja. Realnost je že zdaj »hibridna«, zato ni vprašanje ali se bodo elementi zasebnega in službenega kombinirali ali ne. Vprašanje je kje, kdaj in kako se bodo kombinirali. In seveda kakšno bo pri tem novo ravnotežje med nadzorom in zasebnostjo. ■



Tisti pogumni in napredni delodajalci, ki ta trenutek drzno uvajajo koncept BYOD v svojo vsakdanjo prakso tvegajo, da zabredejo v pravno sivino. Meja, ko gre lahko že za kršitev zakonodaje o varovanju osebnih podatkov, je zato nevarno blizu.

gorenje

ENERGIJSKO VARČNI APARATI



sensocare
technology

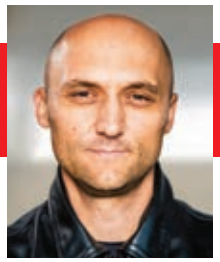
Generacija pralnih in sušilnih strojev Gorenje SensoCare črpa navdih iz potreb uporabnikov, vodijo pa jo mnoga leta izkušenj. Vrhunsko tehnologijo povezuje z estetiko in rezultat je popoln gospodinjski aparat. Zahvaljujoč naprednim tehnološkim rešitvam ter senzorskemu upravljanju smo našli odgovor na ravnanje z različnimi vrstami perila, osredotočeni na varčevanje z energijo ter zaščito naravnih virov pa smo ponosni na visoko energijsko učinkovitost SensoCare aparatov.

DARILO OB NAKUPU! V času med 10. 10. in 31. 12. 2014 ob nakupu izbranega pralnega ali sušilnega stroja Gorenje poleg prejmete darilo, vzglavnik in prešito odejo blagovne znamke Odeja. Za več informacij prosimo obiščite www.gorenje.si.

Gorenje že 8 let najbolj zaupanja vredna blagovna znamka!

www.gorenje.si

Avtorja: Andrej Kovačič / Institut za korporativne varnostne študije*
Alma Ribič, mag. var. / Gorenje group*





KAKOVOST IZVAJANJA STORITEV ZASEBNEGA VARNOSTNIKA PRI VAROVANJU LJUDI IN PREMOŽENJA

V sektorju zasebnega varovanja v Evropski uniji deluje skoraj 10.000 podjetij, ki zaposlujejo okoli 600.000 ljudi. Zasebno varovanje zahteva vedno višjo stopnjo profesionalnosti, s čimer tudi prispeva k razvoju varnejše družbe.

Uvod

Izvajanje dejavnosti zasebnega varovanja zahteva profesionalne pristope k planiranju, izvedbi, nadzoru in izboljševanju procesov varovanja. Za povečanje odgovornosti za kakovost opravljene storitve so pomembni odnosi med zaposlenimi, ki bi morali biti bolj odvisni od profesionalnega položaja in ne toliko od avtoritete. Glavne smernice delovanja so zakonitost, verodostojnost, diskretnost, inovativnost, znanje, spoštovanje, sposobnost sodelovanja in reševanja sporov. Sposobnost sprejemanja nadzora pa je potrebno sprejemati kot priložnost izboljševanja in zavedanja, da profesionalizem prispeva k diferenciaciji zasebno varnostnih družb (v nadaljevanju ZVD) kot tudi njihovih zaposlenih. Zavedati se moramo, da sta profesionalizem in tekmovalnost medsebojno povezana, kar lahko v dobro razvitih profesionalnih sredinah samo še dodatno okrepi funkcije razvoja, validacije in izboljševanja procesov.



Obstajajo razlike glede izvajanja in merjenja učinkovitosti procesov med storitveno in proizvodno dejavnostjo. Veči-

*Korporativna člana Slovenskega združenja korporativne varnosti

V Sloveniji se že vrsto let srečujemo z neko vrsto neskladnosti na trgu varnostnih storitev, in sicer pridobitev poslov ZVD za najnižjo možno ceno, kar posledično pomeni tudi izjemno nizke plače varnostnikov in nižjo stopnjo kakovosti varnostnih storitev.

no orodij za merjenje kakovosti temelji na kvantitativnih meritvah, vemo pa, da se prav vseh postopkov ne da izmeriti zgolj s številkami. Prav to se izraža v storitveni dejavnosti, ki zaradi svoje specifičnosti zahteva druge pristope, predvsem je potrebnega več ocenjevanja in subjektivnosti.

Za obvladovanje delovnih procesov je zelo pomembna kompetentnost zaposlenih. Predvsem je politika upravljanja človeških virov, tudi v ZVD, kazalnik kakovosti in ustreznosti varovanja. Človeške vire je potrebno ustrezno planirati, načrtno usposabljati in strokovno izpopolnjevati, opremiti ter zagotoviti vse potrebne pogoje za kakovostno izvedbo procesov. To pa zahteva ustrezen nivo nadzora, ugotavljanja neskladnosti, analiziranja in seveda ukrepanja ter iskanja možnosti za izboljšave. Kakovost opravljanja varnostnih storitev je tako v soodvisnosti od zaposlenih in managementa ZVD ter njihove vizije.

V prispevku želimo nakazati možne pristope, ki so potrebni za upravljanje in kakovostno izvajanje storitev v zasebnem varovanju.

Kakovost izvajanja storitev v zasebnem varovanju

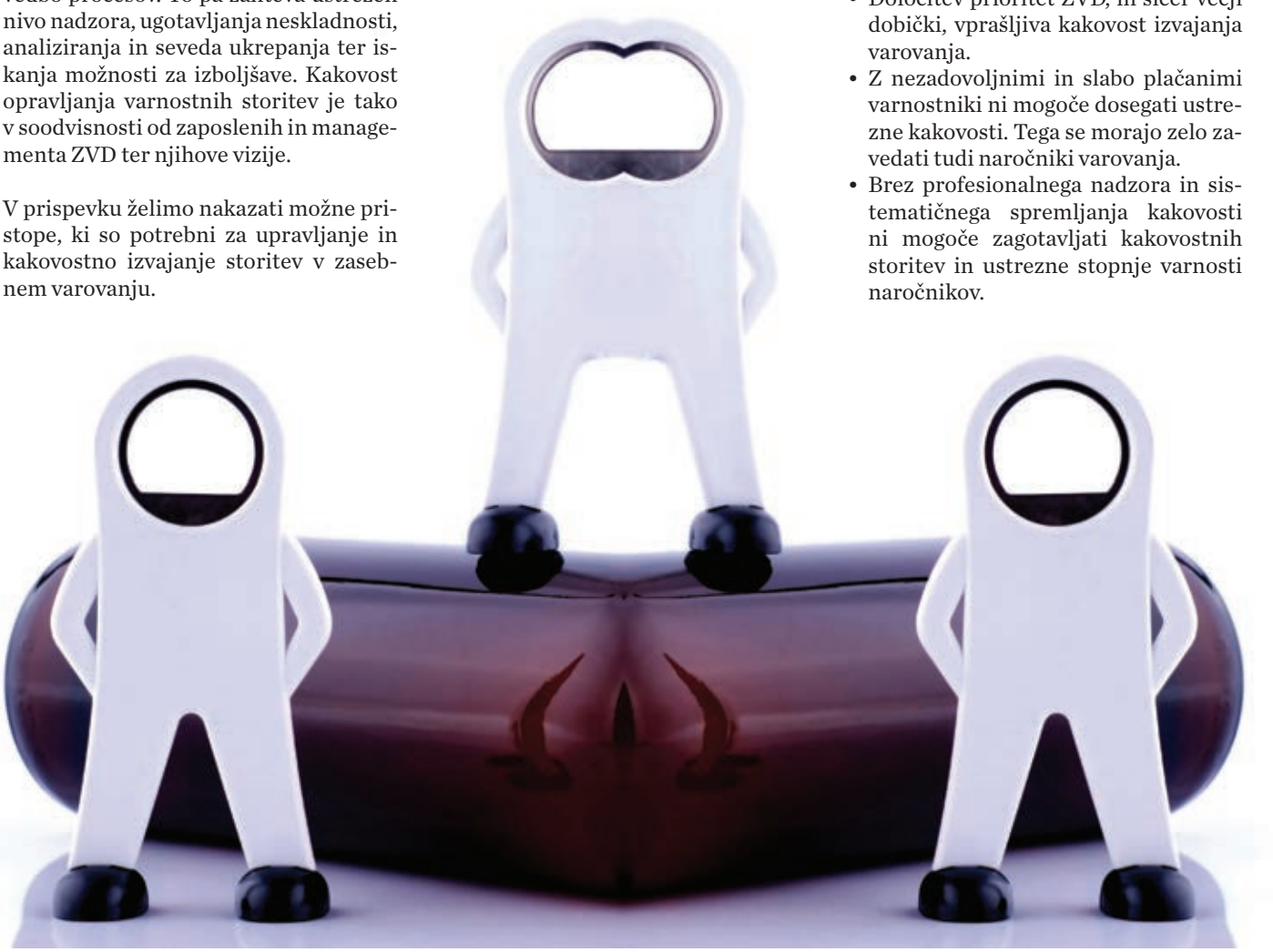
Meriti kakovost v storitveni dejavnosti je težje kot v proizvodnih procesih. Izvajati zgolj varnostne storitve, ali težiti k odličnosti in visoki kakovosti, pomeni delati brez (vidnih) napak in preprečevati ter učinkovito reševati varnostne dogodke. Na kakšen način torej lahko dosegamo kakovost v zasebnem varovanju? Ob upoštevanju določenih značilnosti je kakovost mogoče dosegati na naslednje načine; (1) z izborom kompetentnih kandidatov; (2) z njihovo ustrezno usposobljenostjo; (3) s primernim plačilom za opravljeno delo; (4) z načrtovano strokovno in tehnično podporo; (5) s profesionalnim nadzorom izvajalca in naročnika; (6) z neodvisnim/strokovnim zunanjim nadzorom.

Kakovostno izvajanje storitev varnostnega osebja je pomembno tako za naročnike, kot za dolgoročni obstoj ZVD. V storitveni dejavnosti, kot je zasebno varovanje, so pomembne temeljne karakteristike kakovosti; (1) videz in urejenost osebja; (2) proaktivnost in taktika dela; (3) odzivni čas; (4) komunikacija.

Generalna in trajna odgovornost za zagotavljanje kakovosti je na strani managementa, ki izbira kadre ter organizira strokovna izpopolnjevanja oz. usposabljanja. Najbolj pomembna so interna in ciljno usmerjena usposabljanja, ter pravilne odločitve glede razporejanja varnostnikov na določena delovna mesta.

Pri zagotavljanju kakovosti je tako potrebno upoštevati naslednje:

- Uvajanje standardov kakovosti v zasebnem varovanju.
- Ustrezno planiranje in razvoj človeških virov.
- Določitev prioritet ZVD, in sicer večji dobički, vprašljiva kakovost izvajanja varovanja.
- Z nezadovoljnimi in slabo plačanimi varnostniki ni mogoče dosegati ustrezne kakovosti. Tega se morajo zelo zavedati tudi naročniki varovanja.
- Brez profesionalnega nadzora in sistematičnega spremljanja kakovosti ni mogoče zagotavljati kakovostnih storitev in ustrezne stopnje varnosti naročnikov.



Vloga in naloge odgovornih za dvig kakovosti in ugleda zasebnega varovanja

Vloga države in pristojnih institucij

V shemi nacionalnega varnostnega sistema je zajet zasebno varnostni sistem, katerega del je tudi zasebno varovanje, ki se lahko izvaja pogodbeno/profitno ali neprofitno za lastne potrebe gospodarskih družb. Dejavnost zasebnega varovanja posredno prispeva k skupni notranji varnosti države. S svojimi aktivnostmi in ukrepi hkrati posega tudi v temeljne človekove pravice in svoboščine, zaradi česar obstaja močan javni interes, ki se udejanja v normativno pravnem urejanju in nadzoru s strani države.

V Sloveniji se že vrsto let srečujemo z neko vrsto neskladnosti na trgu varnostnih storitev, in sicer pridobitev poslov ZVD za najnižjo možno ceno, kar posledično pomeni tudi izjemno nizke plače varnostnikov in nižjo stopnjo kakovosti varnostnih storitev. Ker v zasebnem varovanju govorimo o gospodarski dejavnosti, tudi ni moč pričakovati, da bo država ukrepala v smeri določitve minimalne sprejemljive cene varnostnih storitev na trgu. Smiselno pa bi bilo s strani države razmisliti in ukrepati v tistem delu, ko pri javnih razpisih določajo najnižjo ceno kot merilo za izbiro ponudbe, kar bi se v prihodnje spremenilo in bi v razpisnih dokumentacijah bil poudarek na kakovosti storitev in s tem zagotavljanju višje stopnje varnosti. Po podatkih Sindikata Zasebnega varovanja Slovenije KS 90 je v Sloveniji skoraj 7.000 licenciranih varnostnikov zaposlenih pri ZVD, ki se že leta otepajo slabih delovnih pogojev in sramotno nizkih plač. Prav gotovo ima država vse potrebne vzvode za odkrivanje in ustrezno sankcioniranje kršiteljev delovno pravne zakonodaje.

Vloga Zbornice za razvoj slovenskega zasebnega varovanja

Zbornica za razvoj slovenskega zasebnega varovanja ima status reprezentativnega strokovnega združenja na področju zasebnega varovanja v Republiki Sloveniji. Ima tudi pooblastilo za opravljanje nekaterih upravnih nalog, med katerimi je tudi izdajanje priporočil o merilih kakovosti in strokovnosti opravljanja nalog varnostnikov (varnostnega osebja). Zbornica je izdala tudi zloženko na temo, kako izbrati ustreznega izvajalca zasebnega varovanja. Na ta način želijo obstoječe in potencialne naročnike seznaniti z osnovnimi informacijami o zasebnem varovanju in napotilih, kaj naj bo naročnikom vodilo pri izbiri izvajalca varovanja. Omenjena je tudi cena varnostnih storitev, za katero želijo naročnikom povedati, da cena ne more biti edini kriterij pri izbiri, temveč je potrebno pretehtati tudi druge. Opozarjajo, da neupoštevanje vseh elementov, ki izhajajo iz izračuna končne cene (dostojna plača varnostnega osebja, strošek opreme, strošek usposabljanja, in drugi stroški) vodi v nezakonito poslovanje ZVD in ima posledično tudi zelo velik vpliv na kakovost opravljanja storitev. Od Zbornice se prav gotovo tudi v prihodnje pričakuje aktivna vloga pri iskanju rešitev zaradi nevzdržnih razmer na trgu varnostnih storitev.

Vloga naročnikov varovanja

Ali ste se kot naročnik varovanja kdaj vprašali, če je v vaši organizaciji dovolj poskrbljeno za varnost? Ko bo prevladalo pričakovanje in zavedanje naroč-



nikov, da za malo denarja ni mogoče kupiti kakovostnega varovanja, se bodo pričele spremembe v pozitivno smer. Da imajo naročniki urejeno fizično in tehnično varovanje, še ne pomeni, da so poskrbeli za varnost v svoji organizaciji. Z nezadovoljnimi varnostniki v organizaciji naročniki dodatno tvegajo. Zaradi miselnosti naročnikov, da nezadovoljen varnostnik »ni njihova stvar«, sami največ izgubijo.



Ali naročniki res dobijo kakovost, ki naj bi jo z izvajalci varovanja dogovorili, se le-ta lahko spremlja na naslednje načine:

- Z interno vodeno evidenco poslovno finančne škode.
- Z analizo (ne)učinkovitosti in (ne) uspešnosti obravnavanih primerov preprečevanja škode premoženja in ostalih varnostnih dogodkov pri naročniku.
- Z redno anketo varnostnikov o zadovoljstvu s plačilom za njihovo delo. Slabo plačani varnostniki so dodatna/potencialna nevarnost za naročnika.
- Na podlagi videza in urejenosti varnostnikov.

Ali ste se kot naročnik varovanja kdaj vprašali, če je v vaši organizaciji dovolj poskrbljeno za varnost? Ko bo prevladalo pričakovanje in zavedanje naročnikov, da za malo denarja ni mogoče kupiti kakovostnega varovanja, se bodo pričele spremembe v pozitivno smer.

- Na podlagi načina komunikacije z naročnikom in odnosa do njegovih strank ter zaposlenih.
- Glede na morebitne pritožbe nad delom varnostnikov.

Vloga zasebno varnostnih družb

Management ZVD ima pomembno vlogo pri kakovosti v zasebnem varovanju. Za doseganje višje ravni kakovosti varnostnih storitev je pomembno to, da so zadovoljni tudi varnostniki. Kljub vsem motivacijskim dejavnikom, je ustrezno plačilo med pomembnejšimi, še posebno sedaj v ekonomsko zaostrenih časih. Nikakor ni dovolj, da je zadovoljen samo naročnik.

Za upravljanje in obvladovanje kakovosti je nujno potrebna interna služba za nadzor pri izvajalcu varovanja. Je pa res, da je v družbah, ki imajo več 100 ali 1000 zaposlenih, kjer je tudi višja stopnja fluktuacije, veliko težje obvladovati kakovost dela zaposlenih. V teh primerih je še toliko bolj pomemben celovit in sistematičen pristop, ki temelji na učinkovitem upravljanju s človeškimi viri.

Zaključek

Da bi učinkovito upravljali in obvladovali kakovost v zasebnem varovanju, je potreben celovit in sistematičen pristop. Pričakovati od države, da bo posegla v oblikovanje/določitev sprejemljive cene varnostnih storitev, ko je še mogoče zagotavljati ustrezno stopnjo kakovosti, se nam zaradi proste konkurence na trgu zdi nerealno. Realna pa obstaja možnost, da bo na trgu, na katerem ZVD ponujajo svoje varnostne storitve, prevladal zdrav razum. To pomeni, vzpostavitev skupnih razumnih pristopov in aktivnosti med ZVD in naročniki za rešitev te nevzdržne situacije na trgu. Uvajanje upravljanja in obvladovanja kakovosti pomeni bistvene spremembe pri načinu vodenja. Za dvig kakovosti v zasebnem varovanju in za večji ugled panoge bi bila potrebna tudi ločitev varnostnikov od čuvajev (vratarjev), ki spominjajo na neke druge čase. Naročnik bi na ta način imel možnost izbire, ali bo najel varnostnike (varnostno osebje) in s tem imel višji nivo kakovosti varovanja, ki bi ga tudi več plačal, ali pa bo imel zgolj čuvaje (vratarje). Res pa je, da zaradi vseh prej naštetih problemov v zasebnem varovanju, ki se reflektirajo na trgu in pri naročnikih, danes veliko varnostnikov bolj spominja na prej omenjeni kategoriji. Dokler ne bo korenitih sprememb, ni moč pričakovati, da bo poklic varnostnika tudi bolje plačan in cenjen.

Viri

- ASIS, (2012). Houston Baptist University Management System for Quality of Private Security Company Operations - Requirements with Guidancem.
- http://www.zrszv.si/Dokumenti/Zlozenka Kako izbrati izvajalca. pdf ■

Avtorji: Zdenko Hriberšek, Direktor Varovanja, varnostni menedžer, Alma Ribič, mag. var., Metod Budna, mag. obr / Gorenje group*





INTERNO STROKOVNO IZPOPOLNJEVANJE VARNOSTNEGA OSEBJA

Živimo in delamo v času ter okolju, ki od nas zahteva nenehno učenje in iskanje najbolj učinkovitih in kakovostnih rešitev za doseganje zastavljenih ciljev. Zaposleni oz. človeški kapital je ključna gonilna sila konkurenčnosti in razvoja, zato je pomembno prispevati k razvoju in napredku vsakega posameznika in delovnih procesov v organizaciji ter poskušati dosegati čim višjo stopnjo zadovoljstva zaposlenih na poti k doseganju zastavljenih ciljev vsakega posameznika in s tem doseganju skupnih ciljev organizacije ter uspešnosti podjetja.

S fleksibilnostjo E-izobraževanja prihranimo

Postopki planiranja človeških virov izhajajo iz rednega ugotavljanja ustreznosti števila zaposlenih in njihove strokovnosti za potrebe dela, ugotavljanju optimalne izrabe sposobnosti zaposlenih, načinu pridobivanja ustreznega kadra za prihodnje potrebe idr. Planiranje človeških virov je tesno povezano z izobraževanjem, s strokovnim znanjem in usposobljenostjo zaposlenih. V podjetjih se je pomembno zavedati vloge izobraževanja in učenja, ki se nanaša na pridobivanje znanja in veščin, potrebnih za prispevanje k delovnemu procesu in h končnemu rezultatu ter neposrednim ciljem podjetja.

Učenje v organizacijah je vrsta procesov, ki potekajo med zaposlenimi in vključujejo način analize problemov, način reševanja problemov, individualno učenje, učenje timov ter učenje organizacije kot celote. Pri procesu učenja so bistvene nove ideje, ki se včasih oblikujejo na podlagi prebliskov ali kreativnosti zaposlenih v podjetju, lahko se tudi prenesejo iz okolja. Nove ideje pa so prav tako oz. so praviloma produkt tega učenja. Ne glede na izvor so te ideje temeljni vzrok za izboljšave v delovnih procesih, v katerih je učenje pomembna, če ne celo najbolj pomembna sestavina. Zavedati se vloge učenja v podjetju je ključno, saj lahko to učenje na dolgi rok prinaša ključne konkurenčne prednosti podjetju. Ni zanemarljivo pozabljanje



Zavedati se vloge učenja v podjetju je ključno, saj lahko to učenje na dolgi rok prinaša ključne konkurenčne prednosti podjetju.

*Korporativni član Slovenskega združenja korporativne varnosti

oz. opustitev tistega znanja, spretnosti, načinov, ki ne vodijo več k zastavljenim ciljem in predvidenim dosežkom.

Informacijska in telekomunikacijska tehnologija je bistven element sodobnih izobraževalnih procesov in sistemov, tudi v podjetjih. Njeno uporabo v izobraževanju označuje pojem »e--izobraževanje«. Pri opredelitvi e-izobraževanja je smiselno razlikovati dve ravni, in sicer e-izobraževanje v širšem pomenu ali delno tehnološko podprto izobraževanje in e-izobraževanje v ožjem pomenu ali celostno e-izobraževanje. Pri delno tehnološko podprtem izobraževanju se uporablja tehnologija le kot ena od dopolnilnih sestavin tradicionalnega učnega procesa (kot nadgradnja npr. klasičnih predavanj, vaj itd.). Celostno e-izobraževanje pa opušča tradicionalne pedagoške modele. E-izobraževanje se označuje tudi kot uporaba multimedijskih tehnologij in interneta z namenom, da se izboljša kakovost izobraževanja zaradi boljše dostopnosti do virov in storitev, pa tudi zaradi prostorsko neodvisne komunikacije in sodelovanja.

V Skupini Gorenje je skrb za načrtovanje in razvoj kariere delavcev vgrajen v sistem temeljnih vrednot korporacijske kulture. Odgovornost zaposlenih za lasten razvoj je postala ena ključnih vrednot. Spodbujajo izobraževalno dejavnost, osebni napredek zaposlenih in tako se omogoča odkrivanje in pridobivanje ključnih zmožnosti zaposlenih, ki podpirajo uresničevanje strateških ciljev Gorenja, d.d. v celoti. Z izobraževanjem, strokovnim izpopolnjevanjem in usposabljanjem, z višanjem ravni formalne in neformalne izobrazbe in znanj se goji skrben odnos do zaposlenih. Politika zaposlovanja, izobraževanja in strokovnega izpopolnjevanja oz. usposabljanja se prenaša na vse zaposlene, ne glede na nacionalno okolje delovanja, z ustreznimi pogoji za strokovni in osebni razvoj. Poslovni procesi se prepletajo in so soodvisni drug od drugega, zato sistemsko mišljenje podpira transparenten, uporabnikom prijazen informacijski sistem. Ta podpira in omogoča soodvisnost in sodelovanje vseh podsistemov, hkrati pa je temelj timskega dela v podjetju. Sistemsko mišljenje, torej zmanjševanje razkoraka med teorijo in realnimi - praktičnimi primeri, problemi, učenje drug od drugega oz. timsko delo ter problemsko orientirano strokovno izpopolnjevanje, je način praktične uporabe znanj s področja dinamike sistemov in temelji na problemsko orientiranem strokovnem izpopolnjevanju.

Zakon o zasebnem varovanju - ZZasV (UL RS, št. 17/2011) opredeljuje obvezno strokovno usposabljanje in izpopolnjevanje varnostnega osebja. Določa, da se mora varnostno osebje obvezno strokovno usposabljati in izpopolnjevati, z namenom pridobivanja in izpopolnjevanja strokovnih znanj in spretnosti po programih strokovnega usposabljanja in izpopolnjevanja varnostnega osebja glede na vrsto dela, ki ga varnostno osebje opravlja na področju zasebnega varovanja. Strokovno usposabljanje in izpopolnjevanje pomeni usposabljanje v programih strokovnega usposabljanja, izpopolnjevanje v programih strokovnega izpopolnjevanja in izpopolnjevanje v programih obdobnega strokovnega izpopolnjevanja. Vsak imetnik licence je poleg ostalih predpisanih izobraževanj enkrat letno dolžan zagotoviti interno strokovno izpopolnjevanje varnostnega osebja glede na vrsto del, ki jih opravlja. To izpopolnjevanje mora vključevati tako teoretična in praktična znanja ter ustrezne preizkuse usposobljenosti. O izpopolnjevanju morajo biti vodene ustrezne evidence, o njem pa mora biti obveščeno tudi reprezentativno združenje.

E-izobraževanje se označuje tudi kot uporaba multimedijskih tehnologij in interneta z namenom, da se izboljša kakovost izobraževanja zaradi boljše dostopnosti do virov in storitev, pa tudi zaradi prostorsko neodvisne komunikacije in sodelovanja.

V Gorenju, d.d. Področju Varovanje je strokovno izpopolnjevanje tako varnostnega osebja kot tudi ostalih zaposlenih opredeljeno že v Poslovniku kakovosti, s cilji kakovosti na področju zaposlovanja, izvajanja stalnega usposabljanja na delovnem mestu ter izvajanja sistema razvoja kadrov in sistema letnih razgovorov, kar je v skladu tudi z vsemi zakonsko predpisanimi standardi. Izobraževanje oz. strokovno izpopolnjevanje in usposabljanje poteka v sodelovanju in soorganizaciji z Izobraževalnim centrom in službo Informatike in telekomunikacij v Gorenju, d.d.

Vseskozi od potrebe po organizaciji službe Varovanja v Gorenju je potekal kontinuiran proces internega usposabljanja varnostnega osebja, npr. skozi različna navodila za delo, redno odpravljanje neskladnosti pri delu, usposabljanje za rokovanje z orožjem s praktičnim preizkusom, gašenje začetnih požarov, pravila varnega in zdravega dela, reševanje in prva pomoč, tečaji tujih jezikov, računalniški tečaji, protokoli, komunikacijske in organizacijske veščine, uporaba telekomunikacijskih sredstev, reševanje iz dvigal, interaktivne delavnice, razgovori vodij z delavci itd.

Po sprejetju ZZasV v l. 2011, ki je predpisal interno izpopolnjevanje varnostnega osebja, smo že do takrat izvajano interno usposabljanje nekoliko »bolj uokvirili« oz. definirali s programom strokovnega izpopolnjevanja, v katerega smo, glede na pretekla leta, dodali več praktičnih vsebin. Priprave Internega izpopolnjevanja smo se lotili sami in ga prvič izvedli leta 2012. Teoretični del izpopolnjevanja je potekal v klasični obliki v predavalnicah. Predavanja so pripravili in izvedli strokovni sodelavci iz Varovanja in tudi drugih poslovnih področij v Gorenju z aktualnimi vsebinami za varnostno osebje. Poudarek je bil na resničnih primerih iz prakse, vsak primer posebej je bil analiziran, podane so bile ustrezne in pravilne rešitve, prav tako je bilo nekaj časa namenjeno razpravi in podajanju idej za izboljšave v procesih. Izpopolnjevanje je vsebovalo vsebine iz fizičnega varovanja, tehničnega varovanja, varnosti in zdravja pri delu, požarne varnosti, trženja in kakovosti storitev, predstavitev varovanja vojaške baze na mednarodni misiji Slovenske vojske na Kosovu in pa izvedbo brainstorminga – tehnike za pridobivanje novih idej za določeno-izbrano področje dela oz. procesa v Varovanju. Določene vsebine izpopolnjevanja so bile ciljno usmerjene k predpripravi na obdobno strokovno izpopolnjevanje in preizkus usposobljenosti varnostnega osebja. Pri tem klasičnem načinu izobraževanja oz. strokovnega izpopolnjevanja je velika prednost neposredni stik predavatelja z udeleženci, prednost je tudi vzpostavitev pristnejšega odnosa s predpostavljenim in med sodelavci, prav tako pa se v razpravi po koncu predavanj lahko pridobijo tudi ostale koristne informacije od varnostnega osebja, ki bi jih bilo v prihodnosti dobro upoštevati.

V letu 2013 je sledila nadgradnja Internega izpopolnjevanja z zunanjimi predavatelji. Lotili smo se selektivnega izpopolnjevanja, kar pomeni, da so bile vsebine pripravljene za posamezne skupine varnostnega osebja glede na vrsto del in nalog, ki

jih vsakodnevno opravljajo, kot so predavanje zdravstvenih strokovnih delavcev varnostnikom, ki varujejo zdravstvene ustanove, kjer so se le-ti seznanili s posebnostmi in ogroženostjo, s katero se lahko srečajo pri svojem delu (npr. varovanje ambulant, ki skrbijo za odvisnike itd.); tečaj varne vožnje za varnostnike intervente, ki vsakodnevno opravljajo intervencije z vozili in prevoz denarja; usposabljanje iz komunikacijskih veščin, namenjeno varnostnemu osebju, ki imajo vsakodnevni opravek s strankami in pa izvedba tečaja samoobrambe z lastnimi usposobljenimi inštruktorji samoobrambnih veščin.

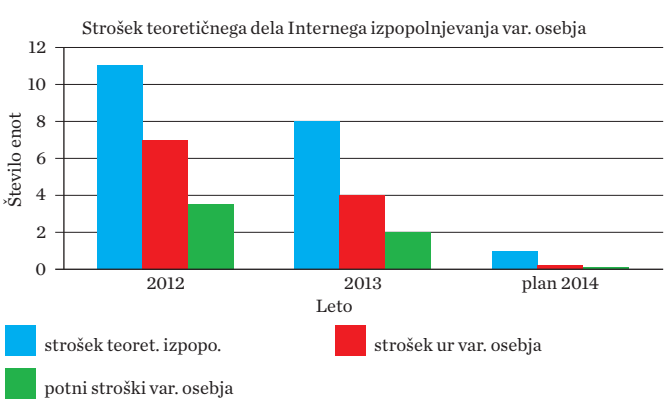
Po analizi internih izpopolnjevanj (primernost, sprejetost pri zaposlenih in njihova pripravljenost za sodelovanje, učinkovitost, stroški itd.) je prišlo do ugotovitev, da so takšna izpopolnjevanja dobrodošla in koristna, so pa stroškovno obremenjujoča za podjetje, prav tako pa se poveča obremenjenost varnostnega osebja z obveznimi dodatnimi urami prisotnosti, ki se jih od njih zahteva.

V trendu po zmanjševanju stroškov na vseh področjih dela, smo se odločili za drugačen pristop k podajanju, prenosu znanja na varnostno osebje, in sicer z uporabo e-izobraževanja. Tu govorimo o E-izobraževanju podjetja Gorenje, d.d. za katerega tehnično in vsebinsko skrbita Izobraževalni center in služba Informatike in telekomunikacij v podjetju. E-izobraževanje kot fleksibilno izobraževanje že vrsto let uspešno omogoča zaposlenim dostop do različnih izobraževalnih vsebin, med njimi je tudi nekaj takšnih, ki so primerne in aktualne za varnostno osebje. Strokovni sodelavci Področja Varovanje so v ta namen pripravili pisno gradivo ter vprašalnike za preverjanje znanja. Pisno gradivo z vprašanji za preverjanje znanja se je vneslo v ustrezno aplikacijo in vstavilo na portal E-izobraževanja na Intranetu Gorenja, do katerega ima varnostno osebje prost dostop. Po pregledu in seznanitvi z vsebinami morajo zaposleni svoje znanje preveriti z elektronskim testom, ki vsebuje 10 vprašanj, pri vsakem poskusu reševanja drugače generiranih, z omejitvijo največ treh poskusov, prag uspešnosti pa je 60%. Tako pridobljeni rezultati preverjanja znanja so priložnost za nadaljnje analize in ugotavljanje, katere vsebine bi bilo potrebno bolj podrobno predstaviti, kje so številčno »največje luknje« v znanju, prav tako se lahko ugotovi posameznike, kateri bi morebiti potrebovali dodatno klasično obliko strokovnega izpopolnjevanja. Vsebina in rezultati testov udeležencev izpopolnjevanja bodo eden od kriterijev za sestavo programa strokovnega izpopolnjevanja v naprej v smislu dograditve oz. s poudarki na vsebinah, kjer je opaziti določeno nepoznavanje ali pomanjkanje glede na želje in ciljno postavljen nivo (vso varnostno osebje mora uspešno opraviti preizkus znanja, s povprečnim rezultatom več kot 80%).

Glede na plan stroškov in delne obračune v letu 2014 za izvedbo teoretičnega dela Internega izpopolnjevanja varnostnega osebja ocenjujemo, da so letošnji stroški precej nižji od stroškov izpopolnjevanja v preteklih letih, in sicer približno za 80%.







Tako kot klasična oblika izobraževanja ima tudi e-izobraževanje svoje prednosti in tudi nekaj slabosti. Prednosti e-izobraževanja so naslednje:

- Prihranek finančnih sredstev/znižanje stroškov (nadure, potni stroški, predavatelji, nadomeščanje varnostnega osebja za čas izpopolnjevanja itd.).
- Prihranek časa, namenjenega za pridobivanje novih znanj (udeleženci se učijo takrat, ko jim to ustreza).
- Odprava težav, povezanih z organizacijo izobraževanja/izpopolnjevanja za večje skupine.
- Stalno sledenje napredku učenja.
- Ni zgornje meje udeležencev izobraževanja.
- Možnost nadgradnje in posodabljanja e-izobraževalnih vsebin.
- Dostop do znanja ni omejen in možnost obnavljanja znanja.

E-izobraževanje tako prinaša splošne koristi za podjetje in zaposlene v procesu izobraževanja, kot so prihranek časa, znižanje stroškov, doslednost podajanja vsebin, večji učni uspeh, možnost obnavljanja pridobljenega znanja, večja kakovost izobraževanja itd. Omeniti moramo tudi koristi za zaposlene, kot so manjša psihološka obremenitev, večja motivacija, uporaba sodobnih informacijskih orodij, enostavna dosegljivost izobraževalnih vsebin idr. Seveda pa je tudi pri tem načinu nekaj pomanjkljivosti, ki jih velja omeniti. Prva in največja pomanjkljivost je pomanjkanje neposrednega, pristnega stika z zaposlenimi. Zaradi tega je pomembno sodelovanje strokovnih sodelavcev, na katere se lahko v primeru kakršnihkoli vprašanj zaposleni obrnejo in skupaj z njimi iščejo ustrezne rešitve. Pri tem je v veliko pomoč tudi sistem letnih razgovorov, ki vzpostavijo neposreden dialog med zaposlenim in nadrejenim. Ostale pomanjkljivosti, ki smo jih zaznali so odlašanje izobraževanja s strani manj motiviranih zaposlenih, neveščost oz. pomanjkljivo znanje na področju uporabe sodobnih informacijsko komunikacijskih poti, predvsem starejših zaposlenih itd.

V poslovnem sistemu Gorenja in pri zunanjih pogodbenih naročnikih je Področju Varovanje zaupana skrb za varovanje ljudi in premoženja v oblikah in načinih, ki jih predpisuje ZZasV. Ker smo storitvena dejavnost, je še kako pomembno zaveda-

nje, da je dodana vrednost vsakega zaposlenega v znanju, ki ga pridobivamo skozi oblike vse učečega podjetja. Zato smo v naši Politiki kakovosti med drugim zapisali: »Zavedamo se, da je zadovoljstvo odjemalcev varnostnih storitev pogojeno z znanjem in zadovoljstvom naših zaposlenih, ki so ustrezno opremljeni in usposobljeni za učinkovito opravljanje svojega dela. Pri tem smo uveljavili načelo, da vsak zaposleni odgovarja za kakovost svojega dela, ki mora v celoti zadovoljiti tako odjemalce kakor tudi sodelavce v poslovnem procesu.«

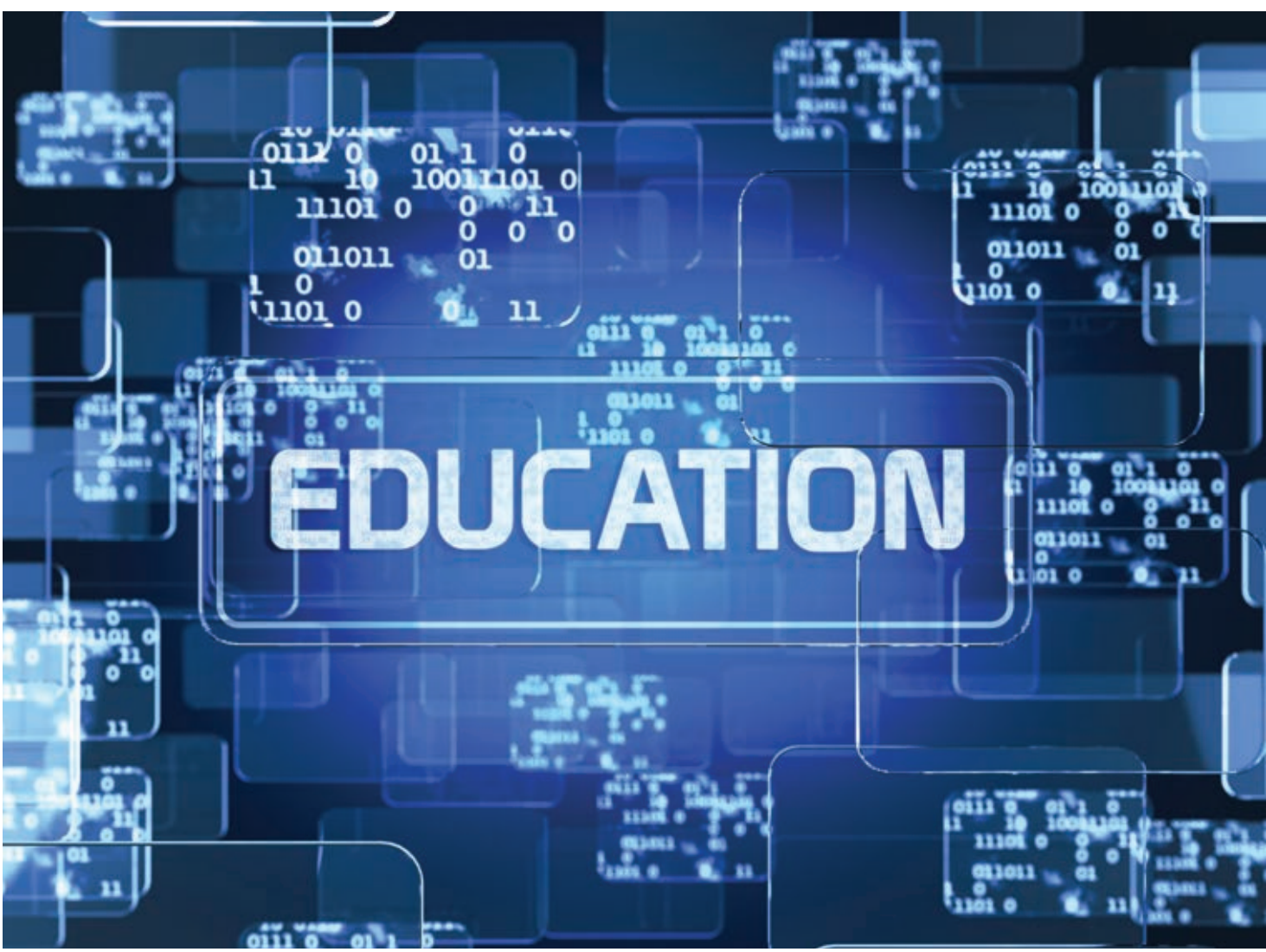
Konkurenčnost storitev povečujemo z nenehnim izobraževanjem/usposabljanjem vseh zaposlenih, saj se zavedamo, da so sedanji časi, kakor tudi prihajajoči, polni priložnosti in izzivov.

E-izobraževanje tako prinaša splošne koristi za podjetje in zaposlene v procesu izobraževanja, kot so prihranek časa, znižanje stroškov, doslednost podajanja vsebin, večji učni uspeh, možnost obnavljanja pridobljenega znanja, večja kakovost izobraževanja itd.

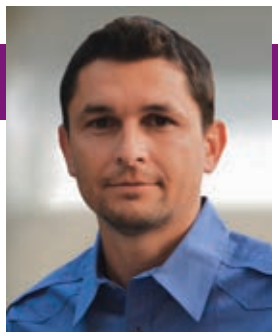
Zavedamo se vseh izzivov, ki jim je izpostavljen poslovni sistem Gorenja, zato se moramo truditi, da smo čim bolj trden člen verige. V tej bitki in nenehni težnji po zmanjševanju stroškov bi imelo opustitev izobraževanja oz. strokovnega izpopolnjevanja zagotovo neželene posledice na strani kakovosti dela, zato smo le-to obdržali oz. ga spremenili v cenejšo obliko. Prednosti in slabosti po SWOT analizi pa so navodilo za uspešno izvajanje internega izpopolnjevanja varnostnega osebja Gorenje, d.d. pri načrtovanju programov izobraževanja s strani vodstva Varovanja in Izobraževalnega centra v Gorenju.

Viri

- Bahun, Drago. Rojc, Emil. Človeški viri – kapital podjetja. Pozoj, Velenje, 2006.
- Kovač, Jure. Sodobne oblike in pristopi pri organiziranju podjetij in drugih organizacij. Moderna organizacija, Kranj, 1999.
- Treven, Sonja. Management človeških virov. GV, Maribor, 1999.
- Uradni list RS, št. 17/2011 z dne 11. 3. 2011: 38. člen ZZasV-1.
- Lea, Bregar. Margerita, Zagmajster. Marko, Radovan. Osnove e-izobraževanja, priročnik. Ministrstvo za šolstvo in šport, Ljubljana, 2010. Dostopno prek: http://arhiv.acs.si/publikacije/Osnove_e-izobrazevanja.pdf, 05.08.2014. ■



Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije-ICS, Ljubljana*



REPORTAŽA:
Nacionalni posvet s področja informacijske varnosti v Državnem svetu

"KIBERNETSKA VARNOST IMPERATIV IN POGOJ ZA ZAGOTAVLJANJE NACIONALNE VARNOSTI"

V hramu slovenske demokracije se je v so-organizaciji Inštituta za korporativne varnostne študije (ICS), Državnega sveta RS, Urada za varovanje tajnih podatkov RS (UVTP) in Nacionalnega odzivnega centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI-CERT) 30. septembra 2014 odvil izredno odmeven nacionalni posvet na temo „Kibernetska varnost imperativ in pogoj za zagotavljanje nacionalne varnosti". Aktualnost obravnavane teme je potrdila povsem polna dvorana, kjer se je zbralo več kot 120 udeležencev.

Posvet so s svojimi nagovori odprli g. Janko Požežnik, Državni svet RS, dr. Denis Čaleta, predsednik sveta ICS, mag. Milan Tarman, UVTP in g. Gorazd Božič, SI-CERT. Poudarili so nujnost sprejema nacionalne strategije za področje kibernetske varnosti, ki nastaja v okviru medresorske delovne skupine na ministrstvu za izobraževanje, znanost in šport.

Na otvoritvi nacionalnega posveta je potekala tudi krajša slovesnost, kjer so bili v Slovensko združenje korporativne varnosti uradno sprejeti novi člani.



V korporativno članstvo združenja so bili sprejeti g. Matjaž Peklaj, Kontrola zračnega prometa Slovenije, mag. Andrej Tomšič, Urad informacijske pooblaščenke RS ter v redno članstvo dr. Brane Bertoncelj, mag. Tomaž Jeretina, mag. Sašo Rakovec, in g. Mirko Šimenko.

V nadaljevanju so cenjeni predavatelji v svojih predavanjih z različnih zornih kotov osvetlili problematiko kibernetske varnosti v Republiki Sloveniji in podali ustrezne informacije o nastajanju nacionalne strategije s področja kibernetske varnosti, ki se trenutno nahaja v javni razpravi. Tako je g. Marjan Turk, generalni direktor Direktorata za informacijsko družbo, skozi temeljno opredelitev aktivnosti na področju uveljavljanju informacijske družbe nakazal mesto kibernetske varnosti. Opredelil je ključne cilje strategije, ki so zagotavljati varnost državljanov, razvoj gospodarstva in družbe in zanesljivo delovanje kritične infrastrukture. Direktor UVTP g. Boris Mohar je podal celovit pregled aktivnosti, ki jih na področju kibernetske varnosti izvajajo različne institucije in predstavil ter poudaril koordinativno vlogo urada v načrtovanem sistemskem ukvarjanju z obravnavano problematiko.

*Član Slovenskega združenja korporativne varnosti



Vodja SI-CERT g. Gorazd Božič je predstavil vlogo centra in skozi praktične primere izpostavil dobre prakse, ki nastajajo v procesu preprečevanja kibernetskih tveganj. Med drugim je izpostavil, da omenjena strategija ne sme biti utopična, slediti ji mora ustrezen akcijski načrt. Poudaril je nujnost ustanovitve nacionalnega laboratorija za preiskovanje škodljive kode. Vodja Centra za računalniško preiskovanje na Upravi kriminalistične policije g. Toni Kastelic, je predstavil grožnje računalniškega kriminala in preprečevanje kibernetskih tveganj s strani organov pregona. Glavni cilj kibernetskih kriminalcev naj bi bili podatki, ki imajo tržno vrednost in kot taki napadalcu prinašajo finančno korist.

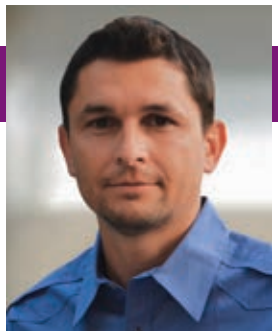
V nadaljevanju je dr. Vojko Podlogar, Ministrstvo za obrambo predstavil semantične in pravne vidike obravnave modernega fenomena, ki ga prinašajo kibernetska tveganja in jih še posebej povezal z vidiki obrambnega področja.

V zaključku je g. Blaž Ivanc, mag., vodja ICS Centra za informacijsko varnost in raziskovalec IJS izpostavil nekaj ključnih ugotovitev in predlogov na področju zagotavljanja obvladovanja informacijskih tveganj v gospodarskem sektorju.

Skozi razpravo, ki jo je usmerjal dr. Denis Čaleta so svoja mnenja, izkušnje in poglede posredovali tudi udeleženci nacionalnega posveta. Vse pobude so bile zbrane in bodo posredovane izdelovalcem Nacionalne strategije o kibernetski varnosti, ki bodo lahko zadnja spoznanja uporabili za izboljšanje nastajajoče nacionalne strategije. ■



Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije-ICS, Ljubljana*



REPORTAŽA:
Mednarodna konferenca "Korporativna bezbednost u Republici Srbiji 2014"

KORPORATIVNA VARNOST DOBIVA SVOJE MESTO V PODJETJIH NA PODROČJU JUGOVZHODNE EVROPE

Predstavniki ICS-Ljubljana in Slovenskega združenja korporativne varnosti so odigrali pomembno vlogo pri izvedbi 2. mednarodne konference »Korporativna bezbednost u Republici Srbiji 2014« v organizaciji Srbske asociacije menedžera korporativne bezbednosti (SAMKB), Privredne komore Beograda, Nacionalne vozačke akademije (NAVAK) in South Eastern Corporate Security Association (SECSA).

Na srečanju so se zbrali številni korporativno varnostni strokovnjaki iz Srbije in širše regije. Konferenco so z nagovori odprli dr. Dragan Trivan, predsednik SAMKB in podpredsednik Gospodarske zbornice Beograda, g. Milan Todorović, sekretar MNZ Srbije, g. Marijan Benko, izvršni direktor korporativne varnosti v podjetju Agrokor d.d. in dr. Denis Ča-





leta, predsednik sveta ICS Ljubljana, ki je posebej poudaril pomembnost takih dogodkov za celotno regijo. Ti dogodki predstavljajo možnost združevanja strokovnjakov s področja korporativne varnosti in tako zagotavljajo izmenjavo dobrih praks in najnovejših spoznanj.

V nadaljevanju so bile podeljene nagrade na področju korporativne varnosti v Republiki Srbiji. Zahvalno plaketo za odlično sodelovanje pa je med drugimi prejel član Slovenskega združenja korporativne varnosti g. Andrej Podvršič, EMEA Director of Security DuPont International.

Po uvodnem delu je g. Andrej Podvršič z izvrstnim predavanjem predstavil korporativno varnost v podjetju DuPont International, trenutne prakse, izzive in trende s katerimi se srečujejo v mednarodnem okolju. Poudaril je, da se ključ uspešne korporativne varnosti skriva v treh pomembnih nalogah. Prva je ta, da uprava družbe prepozna varnost kot dodano vrednost in ne kot strošek. Gospod Podvršič opozarja, da je ena od bistvenih nalog managerjev korporativne varnosti v resnici sposobnost prepričati odgovorne, da je vlaganje v varnost prihranek. Druga pomembna naloga je, da se korporativni varnostni management pozicionira čim bližje ljudem, ki odločajo v podjetju, saj je ravno od teh odvisen znesek vlaganja v varnost. Tretja pomembna naloga pa je proaktivno delovanje.

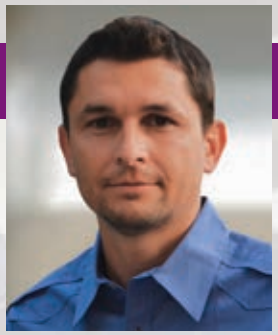
V nadaljevanju sta potekali dve okrogli mizi, kjer so imeli predstavniki Slovenskega združenja korporativne varnosti pomembno vlogo. Na prvi okrogli mizi na temo „ Dinamično varnostno okolje in novi izzivi korporativne varnosti v regiji JV Evrope“, ki jo je moderiral dr. Dragan Trivan, so s svojimi pogledi in izkušnjami sodelovali mag. Miran Vršec, mag. Milan Tarman, g. Marijan Benko, g. Andrej Podvršič in dr. Denis Čaleta. Z razpravami so predstavniki Slovenskega združenje korporativne varnosti pokazali, da so slovenske izkušnje in znanje na zelo visokem nivoju, ter imajo vodilno vlogo pri razvoju področja korporativne varnosti v regiji.

V nadaljevanju je potekala druga okrogla miza, ki jo je moderiral dr. Zoran Keković, sedelovali pa so dr. Goran Matić, sodni izvedenec za informacijsko varnost, dr. Marinko Kresoja, direktor za varnost pri OTP Bank, Dejan Pavlović, namestnik direktorja korporativne varnosti NIS Gazprom NEFT, Vladimir Radović, direktor sektorja za upravljanje s tveganji JP Pošte Srbije in Mladen Raonić, direktor varnosti PTP DIS. Pogovor je tekel o varnostnih izzivih v teh podjetjih, poudarjeno pa je bilo, da korporativni varnostni manager vodi stalen boj med zmanjšanjem proračuna za varnost in držanjem enake ravni storitev.

V popoldanskem delu konference so imeli vsi udeleženci možnost poprijeti za volan novih Toyot Auris, kjer so pod mentorstvom izkušenih inštruktorjev varne vožnje reševali razne težavne situacije na poligonu varne vožnje Nacionalne vozačke akademije (NAVAK).

Konferenca se je končala v prijetnem vzdušju ob izmenjavi mnenj, izkušenj in ob dogovoru, da se taka strokovna srečanja nadaljujejo tudi v prihodnje. Obljuba je bila dana, tako da se dobimo na »Dnevih korporativne varnosti«, največjem dogodku na področju korporativne varnosti v regiji jugovzhodne Evrope, ki se bo zgodil 18. in 19. marca 2015 v Ljubljani. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije-ICS, Ljubljana*



REPORTAŽA:
Mednarodni dogodek v Sarajevu

"ENSURING PERSONAL DATA PROTECTION WHILE SECURING CYBER SPACE"

Konec oktobra je v Sarajevu potekala zanimiva mednarodna konferenca s področja informacijske varnosti z naslovom »Ensuring Personal Data Protection While Securing Cyber Space«. Organizatorja dogodka, ki je potekal v stavbi parlamentarne skupščine Bosne in Hercegovine, sta bila Centre for Security Cooperation-RACVIAC in American University v Bosni in Hercegovini (AU BiH). Soorganizatorji te dvodnevne konference so bili še Ministrstvo za varnost BiH, Ministrstvo za obrambo BiH, Ministrstvo za zunanje zadeve BiH in Vojaška akademija »Mihailo Apostolski« iz Skopja, Makedonije.

Konferenco so svojimi nagovori odprli dr. Danilo Turk, nekdanji predsednik Republike Slovenije; veleposlanik Branimir Mandić, direktor RACVIAC; Igor Rajić, direktor SEECSC; Esmir Ganić, predsednik AU BiH in gospod Tomislav Limov iz Ministrstva za varnost BiH. Med glavnimi predavatelji so bili dr. Brian Woerner, dekan Univerze za računalništvo in elektrotehniko, West Virginia, gospod Brian Bengs, pravni svetovalec v NATO School Oberammergau in dr. Metodi Hadji-Janev, Military Academy »Mihailo Apostolski« iz Skopja.

Na konferenci je bila predstavljena novoustanovljena organizacija South Eastern Cyber Security Center (SEECSC), ki deluje pod okriljem AU BiH. Predstavili so njene aktivnosti, ki bodo prispevale k razvoju zaščite in varnosti podatkov institucij v BiH in širši regiji. Dr. Metodi Hadji-Janev nam je skozi svoje predavanje lepo predstavil različne poglede na človekove pravice in varovanje zasebnosti v digitalni dobi ter izpostavil glavne razlike med pravno ureditvijo EU in Združenimi državami Amerike. Ravno tako smo lahko slišali teme, ki se nanašajo na zaščito zasebnosti in oblikovanja kibernetske varnostne politike, kibernetske vojne, napade preko mobilnih naprav, preiskave kibernetskega kriminala in uporabo podatkov pravosodnih organov. Skozi predavanje g. Briana Bengsa smo lahko spoznali politiko NATA na področju varstva osebnih podatkov v relaciji do zaščite kibernetskega prostora in prihodnjim grožnjam v kibernetskem prostoru.



V nadaljevanju so bile predstavljene izkušnje držav (Albanija, BiH, Hrvaška, Makedonija, Črna gora, Romunija, Srbija in Turčija) na področju soočanja z grožnjami in varnostnimi vprašanji kibernetske varnosti. Regija Jugovzhodne Evrope se sooča s številnimi izzivi na področju varnosti in cilj te konference je bil prispevati k prizadevanjem za reševanje teh težav v prihodnosti. Udeleženci so poudarili pomembnost odprtega sodelovanja, uporabo napredne tehnologije in izobraževanja pri iskanju konstruktivnih rešitev za skupen boj za varnejšo regijo.

Slovenijo so na tem dogodku zastopali že omenjeni dr. Danilo Turk in dr. Denis Čaleta, predsednik sveta Inštituta za korporativne varnostne študije iz Ljubljane. Med povabljenimi gosti je bil tudi slovenski veleposlanik v BiH, mag. Igor Grmek. ■

geacollege
Fakulteta za podjetništvo

Prva generacija študentov že aktivno nabira novo znanje.



MANAGEMENT KORPORATIVNE VARNOSTI

Magistrski program

6. mednarodna konferenca

Dnevi korporativne varnosti

Ljubljana, 18.—19. marec 2015

ICS

Institute for Corporative Security Studies

SPROŠČENO VZDUŠJE, ODLIČNI PREDAVATELJI, MEDIJSKA ODZIVNOST IN PODELITEV NAGRAD SLOVENIAN CORPORATE SECURITY AWARD, IZMENJAVA NAJNOVEJŠIH SPOZNANJ IN DOBRIH PRAKS.

STROKOVNJAKI KORPORATIVNE VARNOSTI, KI VLAGAJO V ZNANJE, BODO Z NAMI.

PRIDRUŽITE SE NAM TUDI VI!

WWW.ICS-INSTITUT.SI